Reference: FOI.ICB-2526/345

Subject: Policies and Governance Documents

I can confirm that the ICB does hold some of the information requested; please see responses below:

QUESTION	**RESPONSE**
I request copies of the following current and applicable policies, procedures, guidance documents, and governance frameworks held by the Integrated Care Board, whether published or internal, including any versions in force during 2024–2025:	
1. Equality, Diversity and Inclusion policy, including any Reasonable Adjustments framework or guidance	Please find enclosed Reasonable Adjustments Guide. Please also refer to: • BNSSG ICB EDI report 2023-24: BNSSG ICS Workforce Equality, Diversity and Inclusion Annual Report 2023 to 2024 • BNSSG ICB Board EDI progress report Oct 25: Update on progress against Equality Objectives • ICB Equality Objectives: Our equality objectives - BNSSG Healthier Together
2. Complaints handling policy and procedures, including escalation and oversight of primary care complaints	Management of Compliments, General Enquiries and Complaints Policy - BNSSG Healthier Together
3. Communication policy or guidance (including accessible communication and preferred contact methods)	https://bnssg.icb.nhs.uk/accessibility-statement/ https://bnssg.icb.nhs.uk/equality-diversity-and-inclusion/accessible-communications/

	https://bnssghealthiertogether.org.uk/library/people-communities-strategic-framework/ - this outlines the ICBs commitment to public engagement
4. Information Governance / Data Protection / UK GDPR policy, including policies covering Subject Access Requests and individual rights	Information Governance Policy - BNSSG Healthier Together Individual Rights Policy - BNSSG Healthier Together Freedom of Information policy - BNSSG Healthier Together
5. Records management policy, including amendment, audit trails, and correction of records	Records Management Policy - BNSSG Healthier Together Records Management Policy Retention Schedule - BNSSG Healthier Together
6. Duty of Candour policy or equivalent “Being Open” guidance	The ICB does not have a Duty of Candour policy.
7. Safeguarding / Vulnerable Adults policy insofar as it applies to disabled or vulnerable patients	Safeguarding adults policy - BNSSG Healthier Together
8. Governance, risk management, and quality oversight policies relating to commissioned GP practices	The ICB has two committees that have quality oversight, these are Outcomes, Performance and Quality Committee and Primary Care Committee. Please see enclosed Quality Management System slides. Please also refer to:

	• Primary Medical Services (PMS) Policy and Guidance Manual (PGM): NHS England » Primary medical services policy and guidance manual (PGM) • NHS Oversight Framework: NHS England » NHS Oversight Framework • Quality Assurance and Improvement Framework (QAIF): NHS England » Professional standards: framework for quality assurance and improvement Robust governance in place through: Quality and Resilience Group Primary Care Operational Group Primary Care Committee
9. Any policies or guidance governing the ICB's role in oversight, intervention, or response where concerns are raised about GP practice conduct or patient safety	B1465-4.-Oversight-roles-and-responsibilities-specification-v1-FINAL.pdf Regarding governance – please see response to question 8. For Primary Care: Dashboard developed that monitors general practice access, quality and resilience, which is monitored through monthly meetings, Patient Safety Strategy and Datix report reviews.
10. Any relevant training policies or mandatory training frameworks relating to Equality Act duties, reasonable adjustments, complaints handling, or information governance	The following documents and frameworks apply (Reasonable adjustments): **Mandatory Training Framework** – Sets out the core compliance training required for all staff, including safeguarding, equality, and

	information governance, ensuring statutory and organisational obligations are met. Aligned with the Core Skills Training Framework and exceeds with internally required courses. **Equality, Diversity and Inclusion Policy and Strategy, and Training** – Provides guidance on promoting inclusive practices, making reasonable adjustments, and ensuring accessible communication for all service users and staff. Required by all staff every three years. **Information Governance/Data Protection Training** – Details how sensitive data is managed, including organisational and individual staff responsibilities, in line with UK GDPR and confidentiality standards. Required by all staff annually. **Safeguarding Adults Policy** – Establishes responsibilities and procedures for protecting vulnerable adults, including mandatory safeguarding training for staff. Safeguarding training ranges from levels 1-5 and requirements are stratified by patient and non-patient facing staff along and then by safeguarding responsibilities. All staff must complete at least level-1 and recertification is required every three years. Safeguarding adults policy - BNSSG Healthier Together Please find enclosed: • IG Acceptable Use Policy • IG Handbook • L&D Policy
Please note: FOI requests and responses are publicly available and therefore personal information has been redacted. The ICB considers the names included in the enclosed document(s) to be personal information and therefore has applied a section 40 (Personal Information) exemption to this information.	

The information provided in this response is accurate as of 26 January 2026 and has been approved for release by Jo Hicks, Chief People Officer/Rosi Shepherd, Chief Nursing Officer/David Jarrett, Chief Delivery Officer, for NHS Bristol, North Somerset and South Gloucestershire ICB.

Reasonable Adjustments

1 Purpose

This document provides guidance when considering reasonable workplace adjustments to enable individuals to work effectively in BNSSG ICB. The document explains the process for applying for a reasonable adjustment, the steps to be taken when considering the request, sources of funding and the recording and monitoring of requirements.

The guidance supports BNSSG ICB to comply with its legal duties and to help meet its aspiration to be an employer of choice. Whilst it is important to consider the legal context, putting in place some simple adjustments can have a positive impact on the wellbeing, experience and performance of the workforce.

2 Principles

BNSSG ICB will:

- Start from an assumption that requests for adjustments are reasonable
- Make balanced final decisions based on the impact an individual adjustment will have on the person as well as the organisation, the requirements of the adjustment, the working environment, tools used and cost
- Act in a timely manner to include the onboarding of new starters who may have needs which require specialist input (e.g. Access to Work Assessment for which there is a known waiting list)
- Put in place temporary arrangements where practical and continued review
- Maintain regular communication with individuals
- Uphold ICB values

3 The Scope of Reasonable Adjustments

The Equality Act 2010 places a legal obligation on organisations to provide reasonable adjustments to ensure that disabled people and those with recognised medical conditions are not disadvantaged in service provision or employment. The aim is for all staff to be treated in an equitable way.

Ensuring equality requires treating people according to their unique needs and is not just about treating everyone in the same way.

Under the Equality Act 2010, a person is considered to be disabled if they have a physical or mental impairment that has a 'substantial' and 'long-term' negative effect on their ability to undertake normal daily activities.

Some staff may choose not to be registered disabled yet may have similar needs to those who are. The decision about whether to talk about their impairment / condition is a personal choice. We encourage all employees to discuss any barriers they face as this will assist line managers to provide appropriate levels of support, enabling the employee to carry out their role in the workplace.

When working for BNSSG ICB, all staff with health conditions or impairments can be considered for reasonable adjustments to support them during their employment. Many adjustments have little or no cost, are straightforward to arrange and are often a matter of flexibility or developing a creative approach to working practices. Our Hybrid Way of Working supports this approach.

If the need for a workplace adjustment is identified, there is a legal duty for it to be implemented if it is reasonable, for someone who meets the legal definition of disability. However, BNSSG ICB considers it to be best practice to implement reasonable adjustments for any members of staff requiring them.

Line Managers should focus on the barriers any employee – registered disabled or not - faces and whether there are adjustments that can be put in place to remove those barriers, rather than whether or not the barrier meets the legal definition.

Adjustments need to be considered in the context of the working environment: Our Hybrid Way of Working involves a mix of working in hot desking office environments as well as in domestic settings. Standard office equipment is available, and stocks are maintained for issue as detailed in Appendix 1.

There is Government support and funding available upon receipt of a formal assessment for those who are disabled or have a long term condition such via the Access to Work Scheme. However, there can be a delay in such assessments and the impact of the delays must be mitigated.

What is a Reasonable Adjustment?

A reasonable adjustment is a change that has the effect of removing or minimising the impact of the individual's impairment in the workplace so that they are able to undertake their duties. There is no legal definition of what is 'reasonable' as this will depend on the individual circumstances of each case. ACAS suggest that a 'reasonable adjustment' is a change that must be made to remove or reduce a disadvantage related to an employee's disability when doing their job or a job applicant's disability when applying for a job

In deciding whether an adjustment is reasonable you should take into account:

- Effectiveness - the extent to which the adjustment would prevent the disadvantage/barrier.
- Financial and budgetary costs of the adjustment/s
- Practicability of the adjustment/s
- The extent of the level of disruption caused to the employee themselves
- Impact on service delivery and people using services
- Impact on other members of staff
- Health and safety implications

It is the responsibility of the line manager to consider reasonable adjustments. They should discuss this with the employee as soon as it is known that there is a requirement for an adjustment to be made. This includes once the appointment has taken place as part of the recruitment process, and in the on boarding phase before a new starter joins. Managers should use the Reasonable Adjustments Assessment form detailed in Appendix 2 to determine if an adjustment is reasonable. Any adjustments agreed should be documented using BNSSG ICB's Tailored Adjustment Plan detailed in appendix 3.

Although not an exhaustive list, examples of typical adjustments include:

- Flexibility in working practices – i.e. the provision of additional breaks, adjusted start/finish times, working from different locations, distribution of duties.
- Providing reasonable time off for assessment, rehabilitation, treatment or counselling.
- Adjustments to systems and processes in place
- Providing information in accessible formats
- Acquiring new, recycling or adapting existing equipment
- Allowing extra time for reading or written work
- Provision of a reader, interpreter or signer
- An adjustment or modification to working environment or premises
- Appropriate communication methods, for example providing written instructions for someone whose anxiety affects their memory
- Providing additional training as required
- Providing additional supervision or mentoring
- Adjusting trigger points for attendance management with advice from occupational health
- Offering appropriate adjustments during recruitment, selection and promotion processes

4 What is a Tailored Adjustment Plan?

A tailored adjustment plan is a live document that helps and supports staff – disabled or not - and their managers to explore options for accommodating adjustments in the workplace. The purpose of the plan is to be "a living document" It should be reviewed regularly and travel with the staff member to whatever role or position they have within BNSSG ICB.

The staff member completes the plan when they know that they need an adjustment/s or need a review of any adjustments that are already in place. The plan can be completed with the support of their line manager if the staff member prefers. As it is designed to be portable, staff members can take their tailored adjustments plan with them to any new job within BNSSG ICB and must review this with their new manager.

Managers will progress the request when they have agreed a workplace adjustment is needed, and will seek help if the complexity is beyond their area of knowledge for example through Occupational Health or Access to Work.

Where an Access to Work referral is likely to cause a delay, Managers must take timely interventions to mitigate the impact. This can include the staff member sharing details of previously supplied equipment up to a total value of £1,500 which can be purchased by BNSSG ICB with approval from the Chief People Officer. The staff member is very likely to know better than most how their condition affects them and may have suggestions for adjustments that should be considered in the interim and ongoing.

The purpose of the Tailored adjustment plan is to:

- Record any agreements about workplace adjustments between a staff member and their Line Manager
- Minimise the need to re-negotiate adjustments each time the staff member is allocated a new Line Manager
- Provide staff members and their Line Manager with a structure for discussions about workplace adjustments
- Help a staff member's Line Manager to understand how a staff member's impairment / condition or circumstance affects them at work
- Prompt staff and /or Line Manager to seek expert advice (Access to Work, Occupational Health) if required
- Review the effectiveness of any adjustments already in place
- Allow both parties the chance to explain any changes in circumstances i.e. personal or Organisationally

When could the Tailored Adjustment plan be created or reviewed:

- On start of employment (**NOTE:** There are significant financial benefits if Access to Work are involved within six weeks of start of employment – see section 7 below)
- At any regular 1:1 supervision
- At a return-to-work meeting following a period of sickness absence
- On receipt of Occupational Health advice or other specialist advice
- Before a change in job or duties or introducing new technology or ways of working
- If is felt that the adjustments no longer meet the staff member's needs.

5 Implementing Reasonable adjustments

The most proactive way of agreeing a reasonable adjustment is through discussion with the employee to determine the options that they believe might be most appropriate and effective. This can include understanding equipment that has been provided previously for staff through Access to Work. Discussions may be between the line manager and the employee and cover the following steps:

1. **Difficulties identified/disability established**: the employee may find it useful to review the Tailored Adjustment Plan to help structure the conversation with their line manager.
2. **Sources of support/advice**: Once the difficulties /disability have been established through conversation, identify what sources of support may be needed or specialist advice required for example via Occupational health or Access to work if required.
3. **Adjustments identified:** Reasonable adjustments assessment completed
4. **Decision regarding the reasonableness of the adjustment**: Tailored adjustments agreed and recorded, or escalation to Director and Chief People Officer
5. **Reasonable Adjustments in place:** Includes sourcing and implementing
6. **Review:** Adjustments reviewed on a regular basis

The standard processes to follow to implement reasonable adjustments can be found in Appendix 4.

7. Access to Work assessments and the provision of equipment

Access to Work (ATW) is a publicly funded employment support grant scheme that aims to support disabled people to start or stay in work. It can provide practical and financial support for people who are disabled or have a long term physical or mental health condition. Support can be provided where someone needs support or adaptations beyond reasonable adjustments.

For staff to be eligible for ATW support they must:

- be disabled or have a long-term health condition that means they need an aid, adaptation or financial or human support to do their job
- have a mental health condition and need support in work

ATW pays up to 100% of the approved costs for adaptations and equipment for employees who have been in the job for less than six weeks, therefore it is important that recruiting managers / line managers draw attention to ATW services on offer of employment and discussing Access to Work and/or reasonable adjustments with the new employee. This should be done in a comfortable, confidential environment and promptly.

For employees who already work for BNSSG ICB, the grant is up to 80% of the approved costs (over and above the £1000 threshold). ATW may be able to pay a grant towards all or some of the additional costs associated with the provision of adjustments required. BNSSG ICB may need to share the cost with ATW if the staff member has been working for BNSSG ICB for more than 6 weeks when they apply for Access to Work support and will have to contribute to costs for:

- Special aids and equipment
- Adaptations to premises or equipment

Applications to ATW must be made by the individual as the service operates as self-referral only. Line managers can support new staff to access this scheme and should prompt individuals to selfrefer. If the application is successful ATW will arrange a workplace assessment, after which the employee will receive a full report including any recommendations. BNSSG ICB will receive a letter confirming the grant awarded, the recommendations and the proportion of the costs Access to Work are prepared to pay. To avoid any delays in process please can the contact details on the application form be addressed to the HR team and line manager. If the Line manager receives confirmation of the grant please can a copy of this letter be forwarded to the People Manager.

On receipt of recommendations from ATW a line manager may wish to consult with their Director / People Support to consider feasibility and effectiveness of the adjustments.

Once agreed, the recommendations should be shared with the People Team, bnssg.reasonableadjustments@nhs.net, who will source items. It is important that there is a clear description of the specific type of equipment required and its availability from suppliers. They should also be told if ATW will provide some funding.

Even where ATW are not involved and there is a specific requirement for equipment it is still important that the requirement is accurately specified, and that financial approval is confirmed. Within BNSSG ICB there is limited expertise in this subject area.

In some cases ATW may identify that equipment must be part funded by the member of staff because it is for personal as well as work related use. BNSSG ICB finance will arrange retrieval of this contribution from the individual.

Where an Access to Work referral is likely to cause a delay, Managers must take timely interventions to mitigate the impact. This can include sharing details of previously supplied equipment up to a total value of £1500 which can be purchased by BNSSG ICB with approval from Chief People Officer. Where this is the case, the exact requirements must be shared with corporate services with the request deemed to be authorised for the commitment of the funds. A line manager may wish to consult with their Director / People Support on the appropriateness of the instruction to corporate services to source previously supplied items.

8. Roles and Responsibilities

The employee will:

- Make their Manager aware of a disability, health condition or impairment, which is having an impact upon their work
- Cooperate with their line manager, People Support, Occupational Health and other agencies in considering if adjustments are required and if so finding the most positive option
- Apply to Access to Work for financial assistance with the costs of equipment or additional support where this is required.
- Maintain personal information on ESR so that there is cohesion between information in the Tailored Adjustment plan and ESR e.g. Emergency contacts/Next of Kin
- Share precise details of equipment supplied previously for consideration for supply by BNSSG ICB.

Line Managers will:

- Provide support to employees who have a pre-existing, or acquire a disability, health condition or impairment during their employment
- Create safe spaces to disclose and be proactive in encouraging discussion
- Deal with any disclosed personal information sensitively and with discretion
- Assess reasonable adjustments to enable the employee to continue in their role.
- Review and monitor the needs of the Employee for whom equipment or assistance has been provided on a regular basis.
- Make referrals to occupational health and third parties to support employees in the workplace.
- Co-ordinate the implementation of reasonable adjustments following Access to Work, Occupational Health assessment
- Ensure that the process for funding approval is adhered to, including any escalation to their Director or the Chief People Officer
- Ask all staff on appointment if they have any additional needs as a result of an impairment and/or health condition and where appropriate, complete a Tailored Adjustment plan with the new employee in order to minimise delays to starting work with BNSSG ICB.
- Provide advice on Access to Work and / or make referrals to Occupational health or manual handling specialists.
- Supply precise details of equipment supplied previously to enable corporate services to source the items. This can be up to the value of £1,500 where an ATW referral will introduce unnecessary delay, or where this ambiguity in the type of equipment that needs to be sourced.

Occupational Health will:

- Provide support and will advise on how a disability or health condition might impact on an employee and the adjustments that might enable an employee to carry out their role.
- Complete occupational health assessments with the employee and share the content of the report with the referring manager, including recommendations for further action (if appropriate)
- Advise if the employee is likely to be covered under the Equality Act 2010 due to the nature of their condition or illness

9. Financial Approval

The cost of any adjustments is met by the People Services budget managed by the Chief People Officer. In many cases the costs associated with providing appropriate technology or equipment are relatively small and should be agreed by the line manager to the value of £1,500 and approved by the Chief People Officer. In some instances, Access to Work will assist with a proportion of the costs.

It should be noted that some low value, commonly used stock items are available from corporate services.

Where costs are likely to be significant (over £1,500), the Manager should discuss costs with their Director and Chief People Officer before making any commitment to the employee about what adjustments can be made (using Reasonable Adjustment Assessment form). This can include the purchase of equipment for disabled staff where there is a known delay to ATW referrals up to £1500.

In any event where a reasonable adjustment is unable to be met, this must always be objectively justified and evidenced by the line manager and referred to the Chief People Officer prior to the application being declined.

10. Where implementing a reasonable adjustment is delayed:

The Line managers and employee should seek to ensure that reasonable adjustments are considered and implemented at the earliest possible opportunity. Where a delay is unavoidable, managers should take all possible steps to ensure the time an employee is without their adjustment is kept to an absolute minimum. Where an employee is fit and able to attend work but they cannot be meaningfully employed in their normal role because a reasonable adjustment is not yet in place, consideration should be given to alternative duties for a short period.

In extreme circumstances where alternative arrangements are impossible to implement during the period of delay, paid disability leave should be considered, while the reasonable adjustment is put in place. Managers should first discuss this option with their Director and Chief People Officer, before confirming whether this is the only viable option.

11. Route of Escalation

No request for a reasonable adjustment should be declined unless the refusal is supported by the Chief People Officer. It is the line managers responsibility to escalate matters to the Chief People Officer where they have not been able to implement and not the individuals.

If the employee is dissatisfied with a decision not to provide a reasonable adjustment as advised by the Chief People Officer, they should respond to the Chief People Officer in writing within 10 working days of being informed of the decision. A review panel will be established to review the decision and rationale. This will be led by the Chief Financial Officer / Deputy Chief Executive or the Chief Executive. Independent advice may be sought.

If after reasonable adjustments have been implemented, the barriers to working have not been addressed satisfactorily, the line manager should review the situation with the individual. Further adjustments should be considered using this guidance.

In the event that reasonable adjustments continue to fail, or adjustments are not provided as they are not considered reasonable, adverse impact on performance will be dealt with under the capability procedure.

The employee will be involved at all stages in considering any aspect of their disability and how this impacts upon their role. If at any stage the employee has any concerns they are encouraged to bring this to the attention of their line Manager and/ or People Support.

12. Supporting Employees

Having a disability and facing the barriers to living with an impairment, mental health issue or long-term health condition can be challenging for an employee both personally and professionally. It is important to make sure their working environment is a safe, positive and unprejudiced place to work. It is the line manager's responsibility to ensure their team demonstrate acceptable, respectful and supportive behaviours towards each other in line with BNSSG ICB Values, fostering good relationships between each other and developing and maintaining the positive working culture for all within the team.

Line management policy training will be provided to line manages to ensure that all appointing managers and line managers understand their responsibilities and the overarching ICB responsibilities under the Equality Act 2010 in supporting and meeting the needs of employees with disabilities, impairments and long-term health conditions.

Appendix 1 – Stock Items

Equipment

BNSSG ICB maintains office bases and collaborates with landlords to provide safe and effective working environments. It also expects staff to work from domestic settings in line with Our Hybrid Way of Working and empowers individuals to make decisions with line management on working arrangements.

In our head office base, our desk booking software permits access to use height adjustable desks for those who wish to use such facilities

To support remote working staff are issued with a laptop, and can also obtain an additional screen, headset and office chair

Recognising that some staff will have additional requirements, the following equipment is available on demand from corporate services as they are kept as routine stock items

- Footrest – basic and rocking varieties
- Mouse mats – flat, gel and gel wrist support varieties
- Copy holder for documents
- Dictaphone

Specialist equipment - Can also be provided when supported by a manual handling, occupational health, or Access to Work assessment:

- Keyboards – different sizes, various functions including ergonomic, split and with number pads
- Mouse – various models
- Screen overlays
- Cushions to support posture
- Chairs – to support correct workstation set up and body shape
- Arm supports – to add to basic features on chairs
- Software – various including screen readers

NB. Where there is a known delay in ATW referrals, equipment up to the total value of £1500 that has been supplied previously can be provided by corporate services once precise details have been supplied by the line manager.

Appendix 2 – Reasonable Adjustment Assessment Form

Reasonable Adjustments Assessment Form

The Reasonable Adjustments Assessment Form should be completed by the manager in discussion with the Employee. It has been designed to help determine if requested adjustments are reasonable for BNSSG ICB to action/put in place. The questions are formulated to assist decision making. If the adjustment is deemed to be reasonable after completion of this form a Tailored Adjustment Plan should be completed and recorded and the equipment obtained/ reasonable adjustment made.

There are three parts to making decisions about reasonable adjustments:

1. Deciding if the duty to make a reasonable adjustment is required,
2. Identifying possible adjustments.
3. Deciding which (if any) of those adjustments are reasonable.

(1) Is an adjustment required?

- Is the person disadvantaged or experiencing a barrier at work?
- Are they experiencing this disadvantage/barrier because of disability?

If the answer is '**yes**' to both of these, you then need to make a reasonable adjustment.

(2) What adjustments could remove this barrier?

Think about what would remove the barrier for the individual. Include the employee in this discussion as they may also be aware of what would help them. Obtain advice about what might be available from Occupational Health, AWP or People Support.

(3) Is the adjustment 'reasonable'?

- **Effectiveness** – how well does the adjustment in question remove or at least minimize the disadvantage?
- **Practicability** – how practical is the adjustment? For example, how long will it take to implement, will anyone need extra training, etc?
- **Cost** – for example, how much will it cost, (including schemes such as Access to Work, for example),
- **Impact** – what negative impact might there be to the business, to others, and/or to the needs of BNSSG ICB
- **Risk** – would making this adjustment cause any risk to others? (Note: An adjustment will not be ‘reasonable’ if anyone’s health and safety would be compromised by making that adjustment.)

Ensure that you consider all information available to you when answering the above – for example reports from occupational health, medical professionals, or other workplace assessments – and ensure that you document both your decision-making process and the decision. The boxes below will help you to document a decision.

Reasonable Adjustment Assessment Form

Name of Individual:
Identified barrier and discussion with individual *Enter a brief description of the barrier that has been identified and summarise potential solutions discussed with the individual, how the individual feels about the proposed adjustment in question*
Effectiveness *Detail how effective the adjustment under consideration would be to remove or minimise the identified barrier for the individual*
Practicality *Detail the practicalities of making this adjustment – for example, the length of time it will take to implement or source items; any additional resources needed to implement or maintain the adjustment.*
Cost Detail the cost of this adjustment and how it will be funded. Ensure all sources of funds are considered (such as Access to Work which can provide funds but only in certain circumstances and within a tight time period).
Impact Detail below the possible extent of any negative impacts of these adjustments. For each impact describe the effect that making it could have on others involved and on the business as a whole.

Health and safety risk Detail below the level of health and safety risk of all stakeholders involved in making this adjustment. Itemise the risks associated with each reasonable adjustment. Where there is no risk state ‘none identified’
Additional evidence to support decision List below the evidence that was considered to help reach the decision. You may want to pull on the advice provided from Access to work, Occupational Health or DSE assessment.
Decision and next steps Details of the decision / recommendation made and next steps
Adjustment approved – yes / no If yes, detail next steps If no, explain why it is not considered reasonable (or appropriate) and escalate to the Chief People Officer Director / Chief People Officer decision and approval of budget spend:

Completed by Line Manager	
Job Title	
Directorate	
Dates	

Approved by Director	
Job Title	
Directorate	
Date	
Verified by Chief People Officer	
Date	

Appendix 3 – Tailored Adjustment Plan

Tailored Adjustments Plan

The Tailored Adjustment Plan provides a framework for discussion in relation to reasonable adjustments that may be required to support employees in their work at BNSSG ICB as a result of a disability, health condition or impairment to remove barriers in the workplace which may be preventing them from working to their potential.

The purpose of this Plan is to:

- Ensure that the employee and line manager have a record of what has been agreed.
- Minimise the need to re-negotiate adjustments each time the employee changes jobs, is re-located, or assigned a new manager within the organisation.
- Provide employees and their line managers with a structure for discussions about workplace adjustments.
- plan for when the employee is unwell and needs additional support because of their disability or condition.

This plan is a living record and will be reviewed and updated as appropriate with the agreement of the employee and the manager, this could be:

- at any regular one-to-one meeting,
- at a return-to-work meeting following a period of sickness absence,
- before a change of job, duties or work location, or the introduction of new technology or ways of working, or
- before or after any change in circumstances for either the employee or the organisation.

Employee's name:	
Job title:	
Department:	
Line manager's name:	
This ‘Tailored Adjustments Plan’ is a living record of adjustments agreed between [employee’s name] and [Line manager’s name] .	
Disability: How my impairment, disability or health condition impacts me in my work	

Examples could include: (please delete / add / amend as required)
Causes:

- *My co-ordination, dexterity, or mobility,*
- *My mental health,*
- *My hearing, speech or visual impairment,*
- *My neuro diversity,*
- *My ability to interact socially with colleagues,*
- *Particular working environments (for example open-plan offices),*
- *The need to attend medical or counselling appointments.*

An example of a response might be:

- *'If my role requires me to stand for long periods of time, then this will create a barrier for me due to my co-ordination/dexterity/mobility condition or I find it difficult to navigate through stairways and heavy doors.*

What allows you and helps you to access work, stay healthy and well and be at your best?

(For example having specific equipment, taking regular breaks from your desk, being able to arrange and use a wider parking bay, exercising before or after work or in your lunchbreak, light and space in the office)

Are there elements of your individual working style and preferences that it is worth your manager being aware of?

(For example, benefitting from quiet reflection time prior to meetings, negotiation on deadlines before they are set, a tendency to have particularly high or low energy in the morning or in the afternoon)

What can your manager and team do to support you to access work and stay healthy and well at work?

(For example providing equipment and software, regular feedback and catch-ups, a particular desk location, flexible working patterns, explaining wider organisational developments, agreeing reasonable adjustments)

Please state below what workplace adjustments will support you at work to fulfil your role and responsibilities? Please refer to Access to Work agreement or Occupational Health report if relevant)

• Add proposed adjustments • Add proposed adjustments • Add proposed adjustments	Date implemented

Wellness at work - employees who have fluctuating disabilities or conditions

Are there any situations at work that can impact negatively on your health and wellbeing because of your particular circumstances?

(For example particular noise, conflict at work, organisational change, tight deadlines, something not going to plan)

When you are struggling more with your health and wellbeing or experiencing poorer health how might it impact you at work?

(For example you may find it difficult to make decisions, struggle to prioritise work tasks, difficulty with concentration, drowsiness, confusion, headaches)

Are there any early warning signs that we might notice when you are starting to experience poorer health?

(For example changes in normal working patterns, withdrawing from colleagues)

If we notice early warning signs that you are experiencing poorer health, what could we do? What additional steps or support might be helpful?
(For example, extra catch-up time with your manager, guidance on prioritising workload)
Is there anything else that you would like to share?
Emergency contacts
If I am not well enough to be at work, I am happy for my line manager to contact my Next of Kin as detailed in ESR. Are your Next of Kin details up to date in ESR. (Yes / No)
I will let you know if there are changes to my condition that affect my work and/or if the agreed adjustments are not working. We will then meet privately to discuss any further adjustments or changes that should be made. If you notice a change in my performance, behaviour or attendance at work or feel that these adjustments are not working, I am happy to meet you privately to discuss alternatives.
Line manager – how to support employee
In line with BNSSG ICB's Managing Sickness Absence Policy, Line managers will stay connected with you in order to discuss your wellbeing and provide reassurance. The regularity and frequency of this contact is agreed as per the below:
Who will contact whom?
How will contact be made? (email, telephone, text, [specific video conferencing platform], letter, minicom)
How often? (daily, weekly, monthly)
When? (preferred day, preferred time)
Unauthorised absences from work

If you are absent from work and have not followed the usual procedures for notifying us that you are sick or absent for a reason relating to your disability or condition, we have agreed to do the following:

- We will try to contact you on your mobile and/or
- notify your emergency contacts:

[add/delete as appropriate]

An up-to-date copy of this form will be retained by the employee, line manager and People Support department.

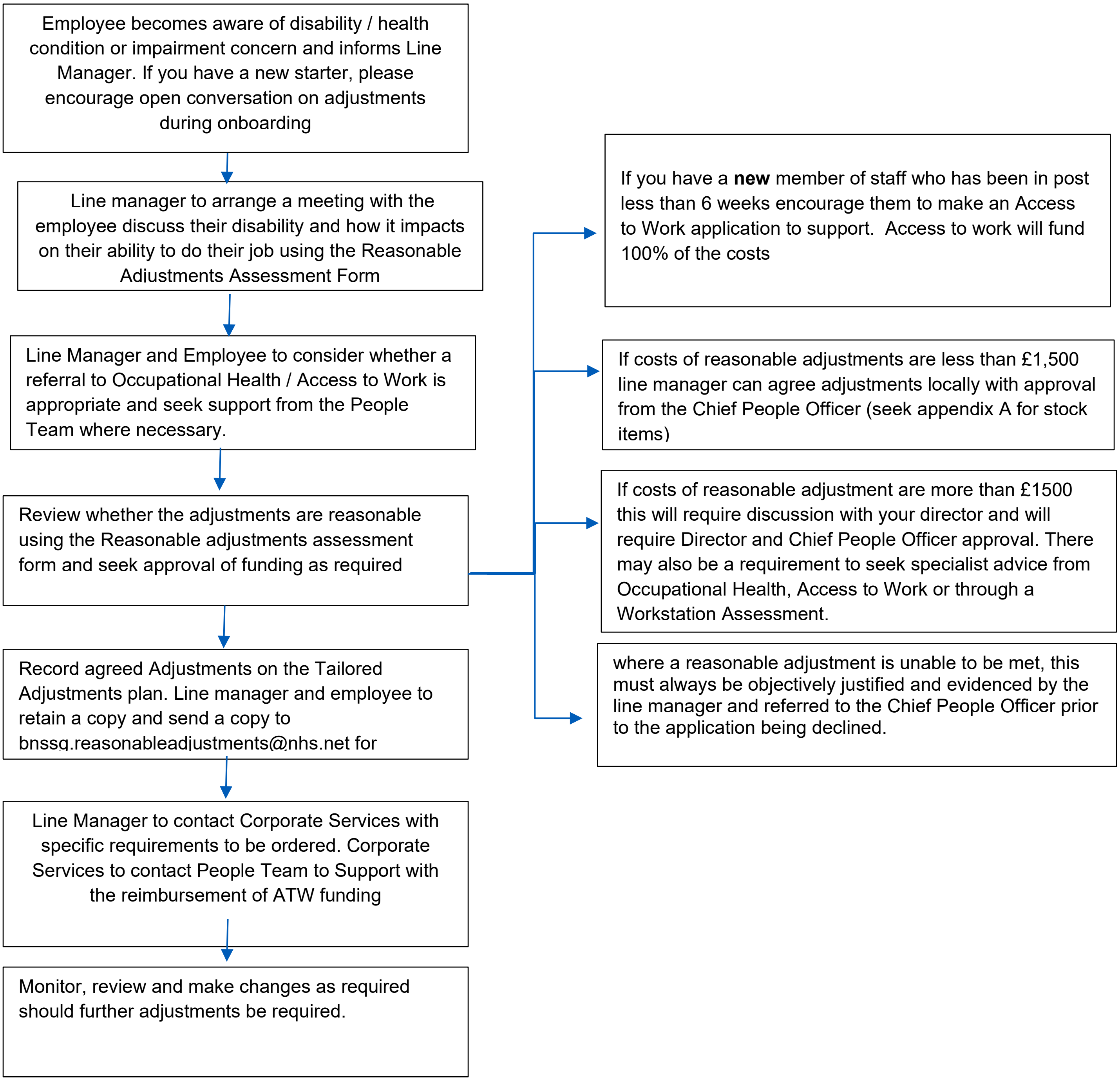
A copy of this form may also be given to a new or prospective line manager with the prior consent of the employee.

Do you have a personal emergency evacuation Plan (PEEP)? Y/N
(If No, contact your Executive PA (Directorate Fire Warden) to discuss requirements and arrangements).

Employee Signature	
Date	
Line Manager's signature	
Date	

Appendix 4

Reasonable Adjustments Flow Chart



Employee becomes aware of disability / health condition or impairment concern and informs Line Manager. If you have a new starter, please encourage open conversation on adjustments during onboarding

Line manager to arrange a meeting with the employee discuss their disability and how it impacts on their ability to do their job using the Reasonable Adjustments Assessment Form

Line Manager and Employee to consider whether a referral to Occupational Health / Access to Work is appropriate and seek support from the People Team where necessary.

Review whether the adjustments are reasonable using the Reasonable adjustments assessment form and seek approval of funding as required

If you have a **new** member of staff who has been in post less than 6 weeks encourage them to make an Access to Work application to support. Access to work will fund 100% of the costs

If costs of reasonable adjustments are less than £1,500 line manager can agree adjustments locally with approval from the Chief People Officer (seek appendix A for stock items)

If costs of reasonable adjustment are more than £1500 this will require discussion with your director and will require Director and Chief People Officer approval. There may also be a requirement to seek specialist advice from Occupational Health, Access to Work or through a Workstation Assessment.

where a reasonable adjustment is unable to be met, this must always be objectively justified and evidenced by the line manager and referred to the Chief People Officer prior to the application being declined.

Record agreed Adjustments on the Tailored Adjustments plan. Line manager and employee to retain a copy and send a copy to bnssg.reasonableadjustments@nhs.net for

Line Manager to contact Corporate Services with specific requirements to be ordered. Corporate Services to contact People Team to Support with the reimbursement of ATW funding

Monitor, review and make changes as required should further adjustments be required.

Appendix 5 – Useful Contacts and Links

Contact	Contact Details
People Team – Reasonable Adjustments	bnssg.reasonableadjustments@nhs.net
People Team – HR	[redacted]
Occupational Health	Accessible via Line Management Referral
Employee Assistance Programme (EAP) Health Assured	HealthAssuredEap.co.uk Username: [redacted] Password: [redacted] Telephone: 0800 030 5182
Access to work	https://www.gov.uk/access-to-work
ACAS	https://www.acas.org.uk/advice Helpline – 0300 1231100
Business Disability Forum (BDF)	Business Disability Forum

Appendix 6 – Frequently Asked Questions

What is a reasonable adjustment?

A reasonable adjustment is an alteration that an employer could make that would enable a disabled person to continue to carry out their duties without being at a disadvantage compared to others. Under the Equality Act 2010, there is a legal duty on employers to make these reasonable adjustments for disabled employees.

What conditions / Impairments are covered by the Equality Act 2010 ?

The Equality Act 2010 says that a disability is a physical or mental impairment, which has a substantial and long-term adverse effect on your ability to carry out normal day-to-day activities. This definition includes impairments or medical conditions such as Cancer, HIV or MS.

A long-term effect of an impairment is one:

- Which lasted at least 12 months, or
- Where the total period for which is lasts is likely to be at least 12 months or
- Which is likely to last for the rest of the life of the person affected.

Effects which are not long-term would therefore include loss of mobility due to a broken limb which is likely to heal within 12 months and the effects of temporary infections, from which a person would be likely to recover within 12 months.

Who can initiate a conversation about a reasonable adjustments?

Normally, it would be for an employee who has a disability or a long-term health condition to speak to their line manager to make them aware that workplace adjustments would be beneficial to them. This may be something that is raised prior to or at the beginning of their employment with BNSSG ICB or it may come up during the course of their employment should they develop a long-term health condition or disability and/or find over time that there may be workplace barriers to them working to their potential.

Line managers should actively be promoting a positive approach towards health and wellbeing within BNSSG ICB and a clear commitment to disability and inclusion. Line managers should encourage their team members to feel more confident about discussing their disability or long-term health condition and encourage employees to talk openly regarding any barriers they are facing, this could be via one-to-ones or in team meetings. This may encourage employees who have not felt comfortable disclosing a disability early in their employment or where they receive a diagnosis whilst they have been in employment with BNSSG ICB to initiate a conversation about workplace adjustments.

What type of support is available to staff with a disability or impairment?

BNSSG ICB will offer a range of support to members of staff. The extent of this support will be dependent on the needs and circumstances of each individual, Not everyone with the same disability/impairment are likely to need the same adjustments. All adjustments will be considered individually. Advice can be accessed via our Occupational Health service provider. Access to Work will also be able to assess an individual within the workplace and make recommendations on what reasonable adjustments.

What is Access to Work?

Access to Work is a publicly funded employment support programme that aims to help more disabled people start or stay in work. It can provide practical and financial support if you have a disability or long term physical or mental health condition.

The support you get will depend on your needs. Through Access to Work, you can apply for:

- a grant to help pay for practical support with your work
- support with managing your mental health at work
- money to pay for communication support at job interviews

How much you get depends on your circumstances. The money does not have to be paid back and will not affect any other benefits you may receive.

Who is eligible for Access to Work?

To be eligible for access to work you must:

- have a physical or mental health condition or disability that means you need support to do your job or get to and from work
- be 16 or over
- be in paid work (or be about to start or return to paid work in the next 12 weeks)
- live and work (or be about to start or return to work) in England, Scotland or Wales - there's a different system in Northern Ireland

You must also:

- already be doing paid work
- be about to start work or become self-employed
- have an interview for a job
- be about to begin a work trial or start work experience under the Youth Contract arranged through Jobcentre Plus

You may also get it if you are getting New Enterprise Allowance.

You can get support from Access to Work:

- however much you earn or have in savings
- at the same time as most benefits, as long as you work more than 1 hour a week

How to Contact Access to Work?

If you are not sure that you are eligible or you want to apply, call the Access to Work helpline.

Telephone: 0800 121 7479
Textphone: 0800 121 7579

Relay UK (if you cannot hear or speak on the phone): 18001 then 0800 121 7479

British Sign Language (BSL) video relay service if you're on a computer - find out how to use the service on mobile or tablet

If phone calls are difficult for you (for example, because you are deaf or hard of hearing), you can ask for all communication to be by email instead.

Or write to Access to Work at:

Access to Work
Operational Support Unit
Harrow Jobcentre Plus
Mail Handling Site A
Wolverhampton
WV98 1JE

Is standard equipment covered by Access to Work?

Access to Work will not pay for equipment that is issued as standard, this should be sourced via the Corporate team, Appendix 1 provides stock items. The employer is also expected to cover the costs of 'reasonable adjustments' that they are required to make under the Equality Act 2010 themselves.

Access to Work will pay for more specialist equipment and support. For example, Access to Work will not issue grants for a standard-issue office chair, but they will consider applications for grants to adapt a standard chair, or a specialist chair that is not issued as standard.

Receiving the recommendations from Access to Work

After an assessment, Access to Work will send written confirmation detailing what adjustments they recommend, and the financial grant amount awarded. They should also suggest where any equipment or services can be obtained.

The line managers with approval from Chief People Officer will share the recommendations with the Corporate team for sourcing. BNSSG ICB can buy the support from any preferred suppliers; they do not need to use those suggested by Access to Work. However, BNSSG ICB will need to make up the difference themselves if the support they purchase costs more than the Access to Work grant amount.

Access to Work will the refund the amount specified in their report to BNSSG ICB.

What happens to the support and equipment if an employee leaves?

BNSSG ICB owns the equipment. This also means that the employer has the responsibility to maintain, insure and dispose of it appropriately. There may be some occasions where BNSSG ICB will allow the employee to take their equipment to their new employer if the employee leaves. If an employee wants to do this, they should agree it with the employer.

If the equipment is donated to the employee, the employer will have to document this as a gift. In other cases, they may sell the equipment to the employee at an agreed price. A 'letter of entitlement' is best practice to prove a transfer of ownership from the employer to the employee.

If Access to Work has funded a support worker, such as a sighted guide or sign language interpreter, the support will stop when the employee leaves their employer. The employee will need to contact Access to Work again if they move to a new job and this support is still required.

Does the employee need to contribute to costs?

There may be occasions where any employee is requested to pay towards costs of an access to work claim if they are using them for personal use. This will be detailed in their access to work grant letter. The employee can appeal the decision and Access to Work will 'reconsider' a grant award, but it limits this to one review. A new Access to Work adviser will carry out the review. It must be the employee who requests this. Access to Work does not use the term 'appeal' due to how the initial decisions are made.

Does a Tailored Adjustment Plan need to be completed in order to receive support?

Understandably some staff may not wish to disclose the nature of their disability or impairment and completion of a Tailored Adjustment Plan is voluntary. The Tailored Adjustment Plan is designed to help support conversations where members of staff are finding that there are things which are making them unable to work to their full potential due to the job design or workplace environment. It is important to note that the legal duty to make reasonable adjustments applies to disabled colleagues experiencing difficulty at work due to their disability regardless of the completion of a Tailored Adjustment Plan.

Appendix 7 – Tips for Managers

When discussing a reasonable adjustments request, remember that the person may feel apprehensive or concerned and it is your role to help them get the most from the discussion by being supportive and offering a safe environment for the discussion to take place.

Plan the meeting in advance giving them enough time to prepare. They may have documents or information that they wish to bring along. This will help them to feel comfortable throughout the process and will help you to make informed decisions based on relevant information and discussion. Take time to review any documents they wish to share with you.

Treat the discussion as confidential and sensitive – you may not need to disclose the adjustments to others in the team and others may not be aware of the issues faced.

Each person’s experience is different and specific to them so take time to focus on their needs and avoid making assumptions or being prescriptive.

Try to understand the impact of their condition/impairment both at work and on them personally and what they hope to get from any adjustments made.

Make sure that you document the meeting and provide the employee with a copy of the notes and any plans or agreements made. This will help in the future when you review their plan and shows that you have listened and understood them.

As a Manager you should:

- Provide clear and straightforward means to discuss and request reasonable adjustments
- (rather than lengthy, bureaucratic processes)
- Be open and available
- Give the employee space to talk
- Avoid interruptions and switch off phones
- Ask simple and non-judgmental open questions such as what, how, when, tell me
- Avoid asking why since this might make the person feel like they are being interrogated
- Speak calmly
- Maintain good eye contact (but be sensitive to neurodiverse individuals who may find this uncomfortable)
- Listen actively and carefully
- Encourage the employee to talk
- Show empathy and understanding
- Be prepared for some silences and be patient
- Seek advice if you need to

- Attend Line Management Policy training for managers and refresher sessions to help aid understanding of managing disability throughout the employment pathway; recruitment and selection, training and development, managing absence etc.

If you feel that the adjustments requested are not reasonable or you are unsure, contact the People Support team for help and advice.

Remember:

- one size does not fit all
- many adjustments are simple and low cost or free
- all agreed adjustments should be reviewed periodically (as agreed)
- it may take time to get used to new equipment/software or to adjust to the changes made

Appendix 8 – Tips for Employees

When asking for adjustments to be made in the workplace it is important that your manager understands:

1. What you are requesting as a reasonable adjustment (what you are asking for)
2. Why you are asking for it (the impact not having the adjustment has on you)
3. How it will improve things for you at work (how things will improve and how much they will improve)

Your manager does not need to know all of the details of any condition that you have but they do have a duty to ensure your safety at work and to do this they need to understand any limitations and the impact of those on your ability to do your job and/or to be in the workplace.

.

In preparing for your meeting, think about the request you have made and how that will have a positive impact on the way you are able to perform at work. Think also of the impact on your colleagues and the wider organisation. Bring along any relevant information that you have such as previous agreements or documents outlining suitable equipment etc.

As an employee you should:

- Be open and honest
- Have time for the discussion to take place fully
- Think about what would help you to be able to fully perform in the role.
- Share any ideas of how you can be supported to work best, in the form of work practices or adjustments

- Discuss how any adjustments agreed are communicated to the rest of the team, if they are communicated at all
- Share any upcoming circumstances which might change the way you work and any support you might need
- Agree how often you would like to check in with your manager to discuss support and adjustments at work, and what form you would like these discussions to take

If you are not happy with the decision following the meeting, speak to your manager first and ask for an explanation of the decision. If you are still unhappy following this you can appeal to the Chief People Officer in writing setting out your reasons for appeal.

Remember:

- One size does not fit all
- All workplaces/workstations are different – even if in the same building
- You will need to keep your manager up to date with any changes in your circumstances or needs
- It may take time for equipment and physical changes to be put in place
- Some items cost more than others so may take longer for funding/approval/arrival
- An easy fix can be implemented quickly – e.g. moving closer to a window
- The more you engage with the process the better able your manager is to assist

Bristol, North Somerset
and South Gloucestershire
Integrated Care Board

ICB Quality Management System

(including mapping of functions of key roles)

[redacted], Deputy Chief Nursing Officer
V.3 May 2024

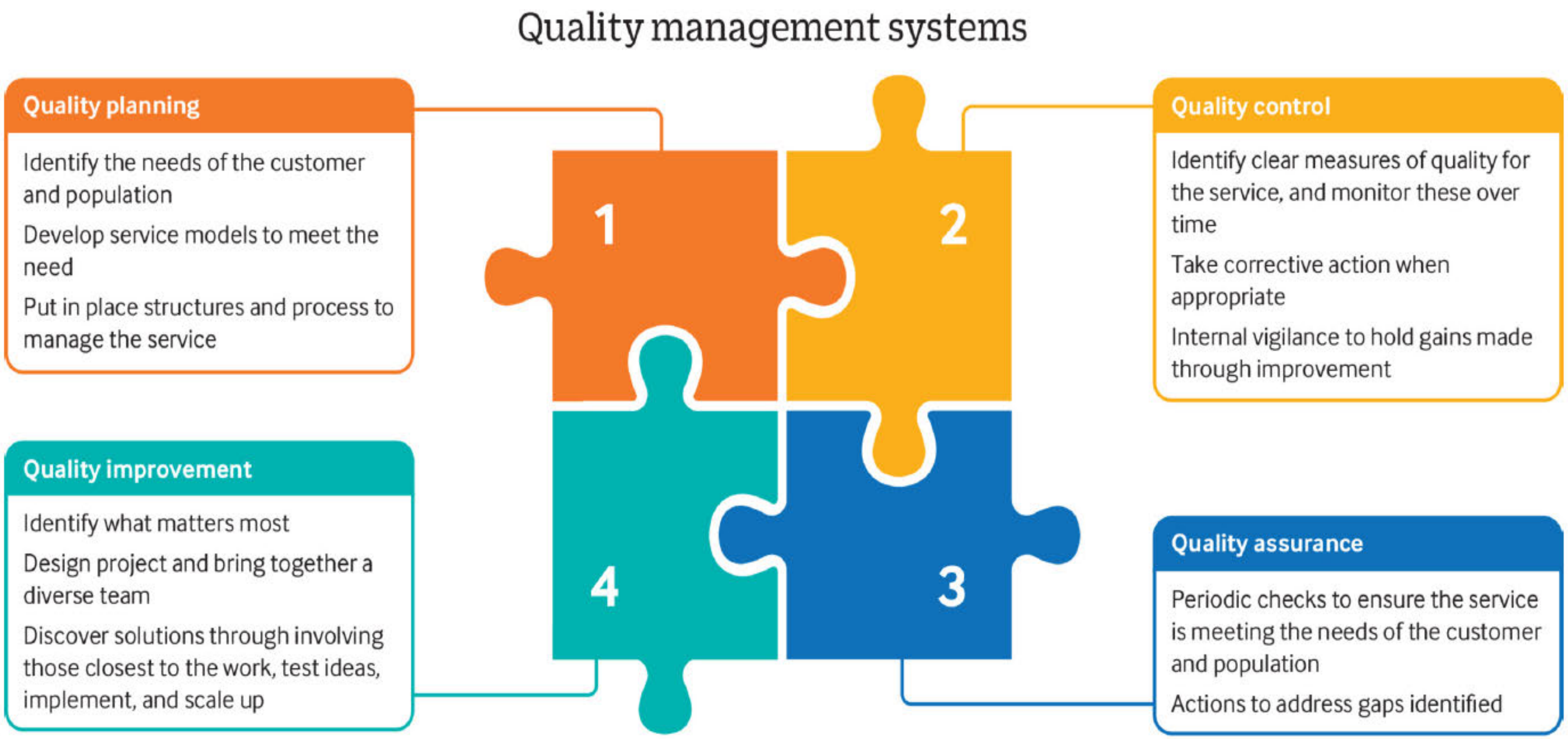
Overview of Quality *Functions* & *Responsibilities* of BNSSG ICB

1. **Strategic quality requirements** – NQB Position Statement and National Guidance on System Quality Groups
2. **Operational quality systems and assurance** – Independent Investigations (including Mental Health Homicides); Regulation 28 reports; Professional Standards; Controlled Drugs Accountable Officer Function; Whistleblowing and Freedom to Speak Up; Quality Accounts; Medicines optimisation; Infection Prevention and Control and Antimicrobial Resistance
3. **Patient safety** - Insight, involvement and improvement (including medical examiners, patient safety improvement priorities, PSIRF, LFPSE)
4. **Experience** – Improving patient, service user and unpaid carer experience of care; insight and feedback
5. **Effectiveness** – National Clinical Audits; NICE technologies appraisals and guidance; GIRFT
6. **Safeguarding** – Safeguarding Assurance & Accountability Framework (SAAF), including Child Protection information System (CPIS) which includes all children on a protection plan (CPP) and looked after children (LAC); child death overview process (CDOP); Child Safeguarding Practice Reviews (CSPRs); Domestic Homicide Reviews (DHRs); Female Genital Mutilation (FGM); Prevent & Counter Terrorism and Modern Slavery & Human Trafficking.

(NHSE Quality Strategy Team – position as of August 2022)

BNSSG ICB
Quality Management System Framework

(Based on - Shah 2020; Kaplan *et al* 2012; Juran 1970)



Quality management systems

Quality planning

- Identify the needs of the customer and population
- Develop service models to meet the need
- Put in place structures and process to manage the service

Quality control

- Identify clear measures of quality for the service, and monitor these over time
- Take corrective action when appropriate
- Internal vigilance to hold gains made through improvement

Quality improvement

- Identify what matters most
- Design project and bring together a diverse team
- Discover solutions through involving those closest to the work, test ideas, implement, and scale up

Quality assurance

- Periodic checks to ensure the service is meeting the needs of the customer and population
- Actions to address gaps identified

Fig 1 | The four aspects of a quality management system: planning, control, assurance, and improvement

ICB Quality functions

(statutory as per NHSE)

Quality Planning

- The ICB is statutorily responsible for delivering functions in a way that secures the continual improvement in the quality of services. Includes commissioning to NICE clinical standards and quality standards, and overseeing and assuring care quality in accordance with the NQB Guidance requirements. These include, ICB exec lead for quality (CNO), a strategy for improving quality, defined governance for identifying, escalating and mitigating risks, defined way to share intelligence (SQG & ICB governance routes),

-- Incorporate local patient safety improvement networks into governance structures in order to develop and implement a system level Patient Safety Improvement Plan.

Quality Control

- Expected that ICBs will have "controlled drugs leads" in place to enable linkages with providers as part of the controlled drugs accountable officer function

- ICB reviews, scrutinises and signs off Quality Accounts from providers; ensures that quality improvement priorities align with system priorities.

- Oversight of ICS and individual provider progress against IPC related ambitions / thresholds / regulatory and contractual requirements / intelligence & improvement programmes.

- Consider key HCAI and AMR surveillance and other data at Place, Provider and ICB levels to understand by pathway what the key factors are that are driving infections. Use this information to inform local priorities and engagement with system partners, to identify where action across a specific infection type, population or Place is required (then becomes Quality Planning)

- ICB to have an identified full time PSS who will also attend System Quality Group

- Medication Safety Officer and a Medical Device Safety Officer to support primary care and ensure good communication and information sharing with the local and national Medication Safety Officer and Medical Device Safety Officer networks respectively.

Quality Improvement

- Oversee and support effectiveness of systems in place in achieving improvement following patient safety incidents; Support co-ordination of cross-system PSIIs; Share insights and information across organisations/services to improve safety and quality

- IPC Improvement Support. Contribute to development of escalation triggers for ICS / regional / national support offer including emerging threats; Support delivery and oversight of regional / national support; Develop ICS level improvement support programmes;

- Responsible for oversight of system safety, to support and work with relevant patient safety improvement networks, patient safety specialists, medication safety officers, other safety leaders, patient safety partners, and the nationally commissioned support function to mobilise improvement activities in response to the Patient Safety Strategy

Quality Assurance

- Support the relevant incident response in relation to all NHS-funded patients in healthcare providers including POD services & indep. Sector; Agree provider PSIRP & policy; FT patient safety specialist (PSS); PSS to support NHS patient safety strategy implementation and improving patient safety at system level (and across care pathways)

- Commission independent investigations responding with oversight to resulting recommendations and assurance again those recommendations

- Respond to system R28 reports (if ICB a named recipient); share learning across ICB footprint from other partners' R28s

-Oversee the quality of POD delegated services through the SW hub function

- Expected that ICBs will have governance leads that will facilitate the development of primary care and designated bodies governance to support Tier 1 & Tier 2 RO responsibilities (medical appraisal and revalidation)

- Oversee the effectiveness of the FTSU cultures within the organisations in their patch – both from a quality and a cultural angle – identify emerging issues and react to them. Disseminating learning across system

- Oversight of Medicines Optimisation through ICS governance structures

- Complaints management (including POD/Primary Care) and dissemination of learning/learning assurance

ICB Quality functions - continued

(statutory as per NHSE)

Quality Planning

- Provide IPC technical and leadership skills to influence ICS and regional policy and direction; Assist providers to translate national policy and guidance to local delivery. Establish and maintain clear structures for IPC & AMR governance, information sharing and escalation with Regional team, partners, and stakeholders; Oversight of provider governance structures

Quality Control

- National Patient Safety Alerts (NatPSAs - ensure local mechanisms exist to support compliance with the actions required in NatPSAs in line with NHS standard contract and national patient safety strategy
- Support providers to transition to the Patient safety incident recording (LFPSE) system; to ensure local recording mechanisms exist to support national patient safety strategy overall aim of continuous increase in effective recording in line with NHS standard contract
- ICB to have clinical digital safety officer in place
- Patient safety thematic analysis of the 'Contact Us' portal - which primary care predominantly utilise to advise ICB of issues/concerns relevant to this service provision

Quality Improvement

- Improving patient, service user and unpaid carer experience of care through co-production - Embed improving experience of care in all quality, improvement and transformation programmes, including coproduction with people with lived experience. Engage with patient experience feedback and metrics
- Reviewing and responding to relevant National Clinical Audits and Patient Outcome Programmes and implementing recommendations.

Quality Assurance

- Support / facilitate medical examiners to provide independent scrutiny of all non-coronial deaths in locality, Support NHSE/I regional medical examiners/ officers in making links between providers in a system.
- Safeguarding Assurance and Accountability - ICB role in oversight of learning and implementation of recommendations from all death reviews and Serious Case Reviews, Child Safeguarding Practice reviews, Safeguarding Adult reviews

Mapping of Quality Team functions Funded Care

Commission care using NHS Short form contracts including a quality schedule.

Contribute and take feedback/learning from CQC meetings with system partners

Arrange contract review meetings as required – planning a forward plan approach to this – undertake an in-depth analysis of quality when staking individuals with specialist needs (MH/LD/EOL) including OOA placements

Review service provision models e/g. Block rounds for EOL to meet population and demand need

- Implementing processes/policies in line with regulatory, IPC/M responsibilities

- Contribution to ICB strategy, Joint Forward Plan, FYFV

- Contribution to nursing/clinical strategy

Personalised care planning

Revised policies - commissioning /choice/PHB /CETR

CHC – framework complaint

Adopting the Bristol Framework for providers Development of place based safety culture

Create a place – based model

Monthly RAGG and FCDG meeting

Start programme of quality review and surveillance with providers, to include presenting regular routine deep dives of areas of patient safety highlighted by partners

Gather intelligence from customer services feedback, patient experience and serious incidents/never events (for above); Healthwatch feedback

Create new quality report for quality and performance metrics to integrate the 4 Health and Care Improvement Groups (HCIGs)

Enacting SOP for escalation of emerging issues/risks/learning to SQG & HCIGs.

-Regular meeting with CQC for all care providers in NS (not replicated in BCC/SG)

Patient feedback – brokerage do follow up call to check quality of care

Patient feedback/survey – expanding the brokerage follow up call to all cohorts

Plan to explore joint quality reviews with LA partners

Developed TOR for decision making – consistency in approach

Refined high cost POC sign off process

[illegible] or enhanced care

Quality Improvement

Implement strategies for improvement based on learning from complaints, incidents, what has gone well – report back via RAGG and OQP

Identify gaps in oversight for those not funded by us

Audit– internal and external - developing a suite of audit that covers all cohorts

Quality Assurance

Produce assurance reports for (and highlight emerging risks) for SQG & associated meetings , ICB Board, OQP, HCPE, system learning panel

Produce, support and coordinate a programme of assurance visits supported by information produced by provider and team (from the other functions detailed in this mapping) – produce KLOEs from intelligence for visits

Oversight of EIA & QIA process for planning of services changes, CIP's and production of EQIAs where appropriate e.g. to articulate system risk, mitigation and gaps in mitigation

Exploring how we gather feedback from care homes and Dom Care providers

Exploring options to review quality of care with Joint funded and PHB individuals

CTR/CETR scrutiny panel being developed

Consider - Develop a quality insight and improvement meeting programme with partner organisations (which will have a workplan for discussion of relevant emerging issues) or quality team members to directly attend provider quality/performance meetings (for direct quality assurance function)?

Mapping of Quality Team functions- BNSSG Medicines Optimisation

Quality Planning

- Oversight of medication optimisation portion of Quality Schedules with providers (annual)

- Support medicines optimisation section of Patient Safety Strategy

-- Contribution to ICB strategy, Joint Forward Plan

- Integrating NHS Pharmacy and Medicines Optimisation (IPMO) Plan across the ICS

-Medicines Optimisation Governance

-Support commissioning to NICE clinical standards and quality standards

- Chair Medicines Safety and Quality group across ICS which meets every 8 weeks

- Work with digital teams to try and resolve some of the issues e.g. lack of interoperability between IT systems

Quality Control

- Review all medication related DATIX reports to gain learning, share with partner organisations and complete thematic analysis

- Create new quality report for quality and performance metrics to integrate the 4 Health and Care Improvement Groups (HCIGs)

- Escalate emerging issues/risks/learning

- Support local mechanisms that exist to support compliance with the actions required in National Patient Safety Alerts (NatPSAs) supported by Medicines Optimisation team

- Numerous Medicines Optimisation Prescribing Quality Scheme (PQS) projects completed annually in Primary Care. Includes achieving financial balance and quality and safety projects

- Medication Safety Officer and Medical Device Safety Officer in ICB works alongside Medication Safety Officers across the ICS

- Lead AMS and support HCAI and AMR surveillance and other data

-Medicines Optimisation links with controlled drugs accountable officer

Quality Improvement

- Lead the identification of Medicines Optimisation QI priorities

- Medicines Optimisation representation at Patient Safety Specialist Advisory Group

- Share insights and information across organisations/services to improve safety and quality

- Send Medicines Quality and Safety quarterly newsletter and Medicines Optimisation monthly newsletter across the ICS

-Support and work with relevant patient safety improvement networks, patient safety specialists, medication safety officers, other safety leaders, patient safety partners, to mobilise improvement activities in response to the Patient Safety Strategy

- Developing pharmacy workforce plans alongside building awareness of medicines optimisation in wider disciplines

Quality Assurance

- Produce assurance reports for (and highlight emerging risks) for OQP, HCPE, GPCB and other required meetings

- Support the relevant incident response in relation to all medication related Datix

-- Oversight of EIA & QIA process for planning of new services/changes and production of EQIAs where appropriate

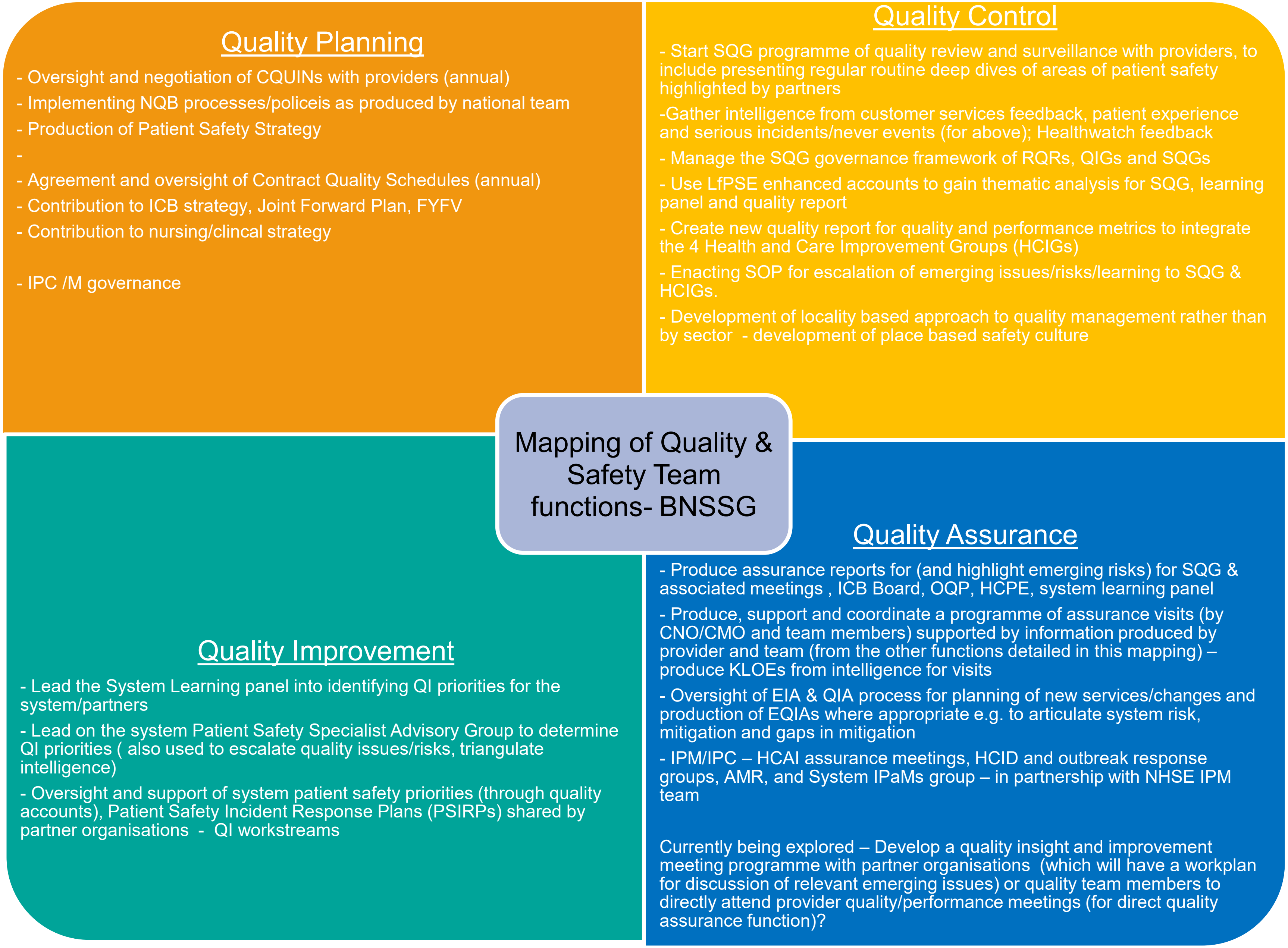
-- Oversight of Medicines Optimisation through ICS governance structures

- Complaints management (including POD/Primary Care) and dissemination of learning/learning assurance

-Risks associated with medicines are managed across a system, including both clinical and financial risk

-Leads APMOC to ensure appropriate governance processes and procedures are in place to assure a safe and high quality decision making process in relation to medicines. This group aims to facilitate national and local guidance and helps to ensure a consistent evidence based approach to prescribing and medicines is taken across BNSSG

Lead BNSSG Joint Formulary Group a collaborative approach to manage the introduction, utilistation or withdrawal of medicines/technologies within the BNSSG Joint Formulary across the ICS



Mapping of Quality & Safety Team functions- BNSSG

Quality Planning

- Oversight and negotiation of CQUINs with providers (annual)
- Implementing NQB processes/policeis as produced by national team
- Production of Patient Safety Strategy
-
- Agreement and oversight of Contract Quality Schedules (annual)
- Contribution to ICB strategy, Joint Forward Plan, FYFV
- Contribution to nursing/clincal strategy

- IPC /M governance

Quality Control

- Start SQG programme of quality review and surveillance with providers, to include presenting regular routine deep dives of areas of patient safety highlighted by partners

-Gather intelligence from customer services feedback, patient experience and serious incidents/never events (for above); Healthwatch feedback

- Manage the SQG governance framework of RQRs, QIGs and SQGs

- Use LfPSE enhanced accounts to gain thematic analysis for SQG, learning panel and quality report

- Create new quality report for quality and performance metrics to integrate the 4 Health and Care Improvement Groups (HCIGs)

- Enacting SOP for escalation of emerging issues/risks/learning to SQG & HCIGs.

- Development of locality based approach to quality management rather than by sector - development of place based safety culture

Quality Improvement

- Lead the System Learning panel into identifying QI priorities for the system/partners

- Lead on the system Patient Safety Specialist Advisory Group to determine QI priorities (also used to escalate quality issues/risks, triangulate intelligence)

- Oversight and support of system patient safety priorities (through quality accounts), Patient Safety Incident Response Plans (PSIRPs) shared by partner organisations - QI workstreams

Quality Assurance

- Produce assurance reports for (and highlight emerging risks) for SQG & associated meetings , ICB Board, OQP, HCPE, system learning panel

- Produce, support and coordinate a programme of assurance visits (by CNO/CMO and team members) supported by information produced by provider and team (from the other functions detailed in this mapping) – produce KLOEs from intelligence for visits

- Oversight of EIA & QIA process for planning of new services/changes and production of EQIAs where appropriate e.g. to articulate system risk, mitigation and gaps in mitigation

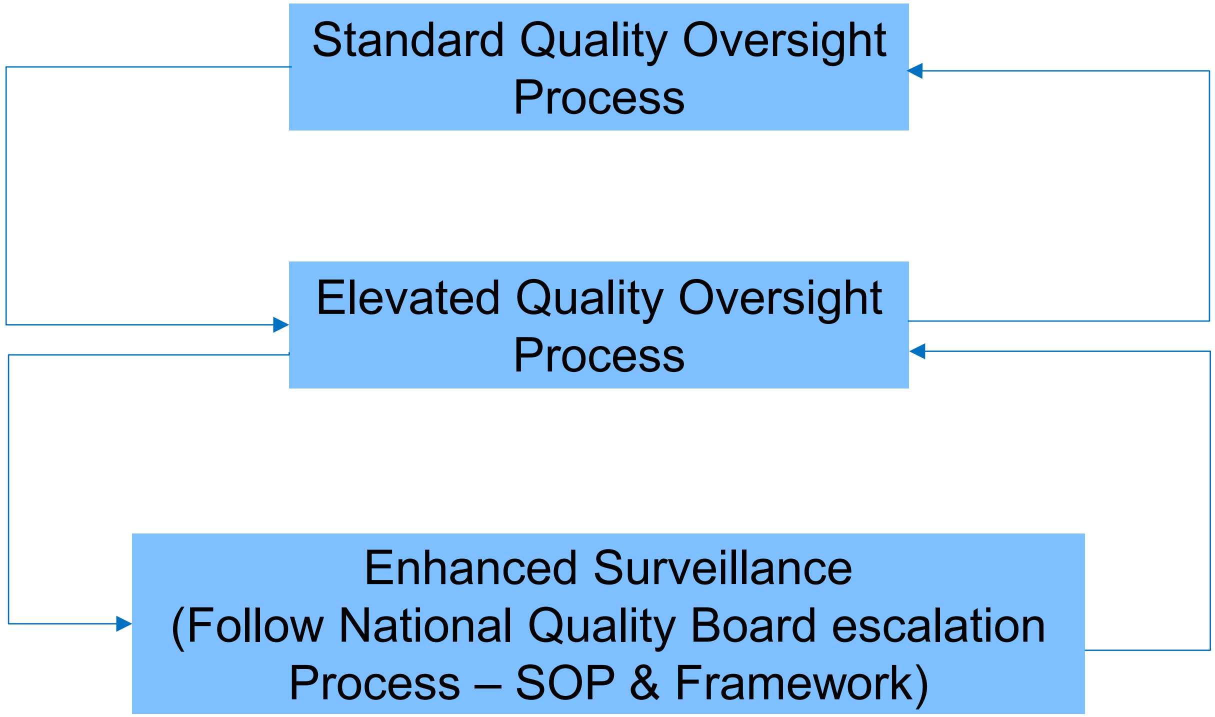
- IPM/IPC – HCAI assurance meetings, HCID and outbreak response groups, AMR, and System IPaMs group – in partnership with NHSE IPM team

Currently being explored – Develop a quality insight and improvement meeting programme with partner organisations (which will have a workplan for discussion of relevant emerging issues) or quality team members to directly attend provider quality/performance meetings (for direct quality assurance function)?

Delivering a Quality Management System Framework within the ICB

Quality, Safety and Safeguarding Contractual Oversight with Providers/Partners

Principles



Standard Quality Oversight Process

Elevated Quality Oversight Process

Enhanced Surveillance
(Follow National Quality Board escalation Process – SOP & Framework)

Standard Quality Oversight Process (for each main provider/partner)

- Yearly agreement of CQUINNS
- Yearly agreement of contract quality schedules
- Annual review and support of partner's quality account
- Quarterly one-to-one meeting of Patient Safety & Quality Lead/PSS with Partner's counterpart Quality Lead, to identify any current or emerging quality issues (for further support or escalation), including S.28s
- Quarterly one-to-one meeting of 8a ICB Patient Safety & Quality Lead with appropriate internal ICB Contracts Manager to review all providers in ICB's Quality Lead's responsibility (driven by HCIG portfolios - see later slides)
- Attendance at relevant SDU related to Quality Lead's/PSS's portfolio for input into quality issues
- Quarterly review of themes and learning from provider's SIs and other PSIRF processes, and identify QI themes for system
- Agree a schedule of 2 visits/year for quality review/deep dives from issues highlighted from standard oversight (including areas for celebration)
- At any time escalate through the Quality Management System Framework (previous slide) any issues that may require Elevated Quality Oversight or Enhanced Surveillance; inform ICB Exec team

Elevated Quality Oversight Process (for each main provider/partner)

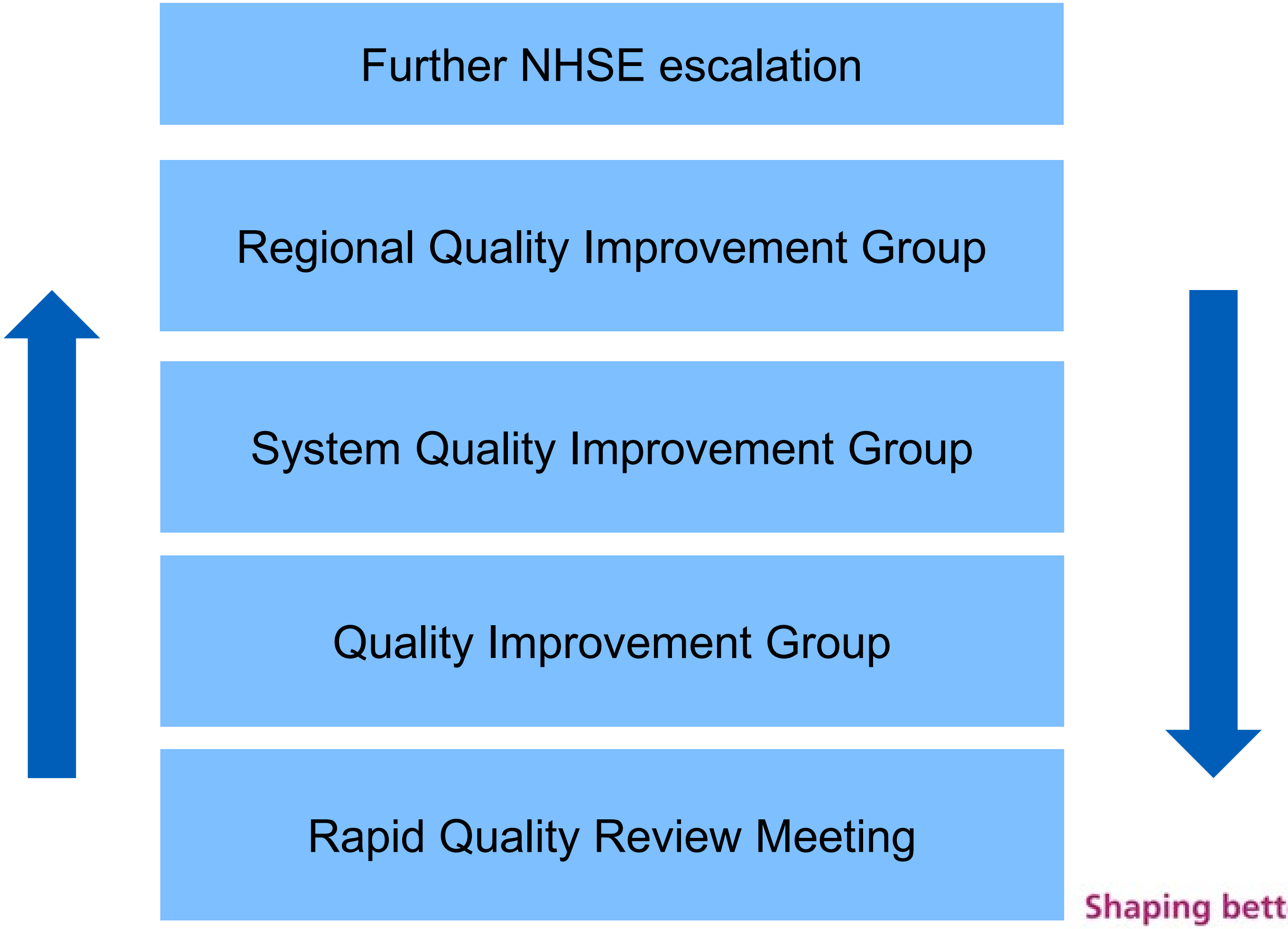
- If issues are determined to be an immediate risk to patient safety, convene a Rapid Quality Review meeting, and follow the process for Enhanced Surveillance
- Enact Elevated Quality Oversight if stepping down from Enhanced Surveillance, or escalation to Enhanced Surveillance is not required following discussions at Rapid Quality Review

Functions of Elevated Quality Oversight:

- Monthly Elevated Quality Oversight meetings chaired by Patient Safety Specialist, with colleagues from quality team and provider/partner. Meeting will seek assurance on progress of agreed quality improvement actions plans, and review and discuss new risks, improvements, successes and challenges
- Produce brief monthly highlight report for System Quality Group (SQG) from the oversight meeting
- Share highlight report with Contracts Team and invite Contract Manager to attend Elevated Oversight meeting if appropriate
- At appropriate time (good progress on action plans) bring recommendation to SQG to step-down to Standard Quality Oversight (business as usual)
- Escalate immediately to a Rapid Quality Review Meeting if progress is deteriorating and it is determined Enhanced Surveillance may be required; inform Exec team

Enhanced Surveillance
(Follow National Quality Board escalation Process – SOP & Framework)

- For further details within these steps please refer to the BNSSG ICB NQB escalation framework paper and SOP



Further NHSE escalation

Regional Quality Improvement Group

System Quality Improvement Group

Quality Improvement Group

Rapid Quality Review Meeting

Quality Management System - Proposed arrangements between Contracts Team and Quality Team for all contracts, including smaller and independent providers/partners (excluding Primary Care)

- Routine Quarterly meeting between ICB Patient Safety & Quality Leads/Manager, Performance and Contract Team Leads/Managers
- Any issues related to providers/partners shared between Quality and Contracts colleagues at the meeting, or escalated urgently between meetings if required
- Quality issues that need escalating to enter Quality Management System Framework and to enter either Elevated Quality Oversight or Enhanced Surveillance (as per previous slides)
- Contracts and Performance team to be members of monthly elevated quality oversight or enhanced surveillance meetings if appropriate, to assist with any contractual/remedial actions required, and to avoid duplication – aim to reduce the number of meetings for both Contracts and Quality colleagues
- Invite CQC locality relationship managers to the routine monthly meetings (to avoid duplication of other meetings)

Quality Management System - Proposed arrangements between Contracts Team and Quality Team for all contracts – partners new to the system (continued)

- General principles –patient choice/any qualified provider arrangements - a risk-based approach will need to be untaken when reviewing new partners entering the market in the BNSSG system
- For those partners new to the system, a quality visit will only be undertaken if the organisation does not have an NHS ICB contract elsewhere in the country
- For those organisations where an NHS contract is already in place, a quality visit will not normally be undertaken.
- In all cases the quality lead (who's HCIG portfolio it equates to) will liaise with the system(s) who already commission the prospective partner, to determine if there are any quality and performance issues – if there are, then a quality review/visit will be undertaken

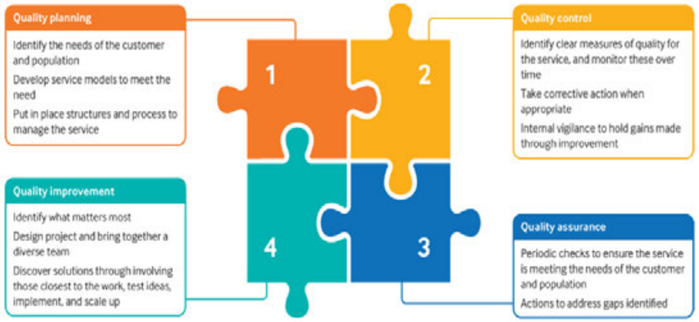
Quality Management System- Proposed arrangements for Primary Care

- Routine Monthly meeting between Patient Safety Specialist and relevant 8a ICB Patient Safety & Quality Lead and Primary Care Contracting Team Leads/Managers
- Any issues related to Practices shared between Quality and Primary Care colleagues at the meeting, or escalated urgently between meetings if required
- Quality issues that need escalating to enter Quality Management System Framework and to enter either Elevated Quality Oversight or Enhanced Surveillance (as per previous slides)
- Primary Care Team to be members of monthly elevated quality oversight or enhanced surveillance meetings if appropriate, to assist with any contractual/remedial actions required, and to avoid duplication – aim to reduce the number of meetings for both Primary Care and Quality colleagues
- Invite CQC locality relationship managers to the routine monthly meetings (to avoid duplication of other meetings)

Quality Management System –
Proposed arrangements for Safeguarding Oversight

Proposed general principles:

- Enhanced Surveillance – ICB Safeguarding representation in whole process where appropriate as per current arrangements
- Elevated Quality Oversight Process – ICB Safeguarding representation at Elevated Oversight meetings and actively involved in process where appropriate, including seeking assurance against improvement/action plans
- Standard Quality Oversight Process – to be determined in March/April 2024 between ICB and Partners using the Quality Planning, Control, Assurance and Improvement framework



Quality planning

Identify the needs of the customer and population

Develop service models to meet the need

Put in place structures and process to manage the service

Quality control

Identify clear measures of quality for the service, and monitor these over time

Take corrective action when appropriate

Internal vigilance to hold gains made through improvement

Quality assurance

Periodic checks to ensure the service is meeting the needs of the customer and population

Actions to address gaps identified

Quality improvement

Identify what matters most

Design project and bring together a diverse team

Discover solutions through involving those closest to the work, test ideas, implement, and scale up

- Arrangements will incorporate the NHSE Safeguarding, accountability and assurance framework (SAAF) and the governance principles of NHS sovereign Providers.
- To include ICB role in oversight of learning and implementation of recommendations from all death reviews and Serious Case Reviews, Child Safeguarding Practice reviews, Safeguarding Adult reviews etc

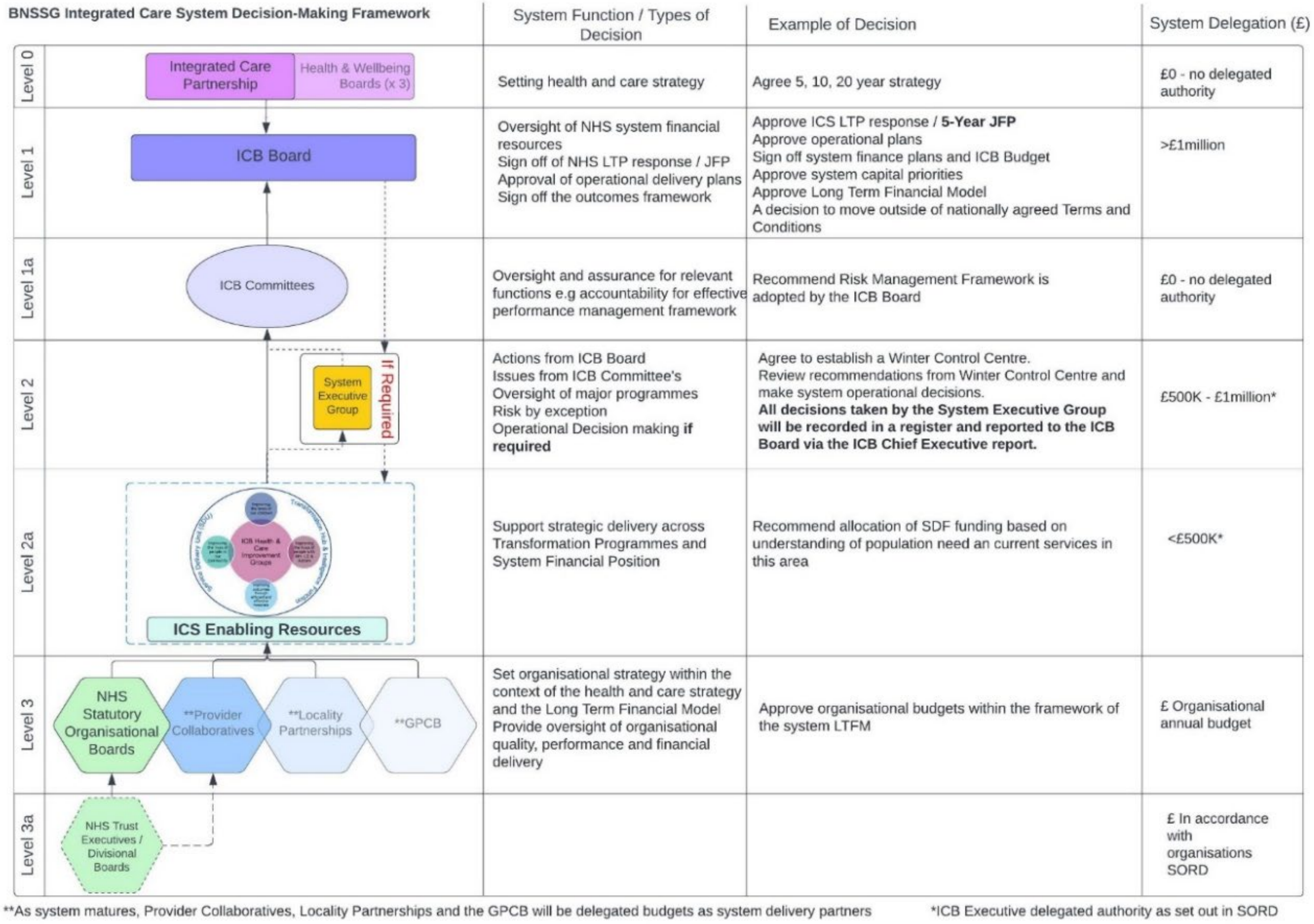
DRAFT Mapping of the Quality Management System roles (including HCIGs/SDUs) and levels of accountability/responsibility

Note, these are elements of the role related to the Quality Management System, and are not reflective of the whole roles/job descriptions of colleagues)

Level	Quality Planning	Quality Control	Quality Assurance	Quality Improvement
Execs (CNO & CMO) (x2)	• Provides leadership and support to the functions detailed below • Outcomes Quality Performance Committee	• Caldicott Guardian • DIPC • Leadership & Oversight of below	• Quality insight visits • Chair SQG & HCPE • Lead/delegated Safeguarding Partner • Outcomes Quality Performance Committee and other committees of the Board	• Leadership & Oversight of below
Deputy Execs (x4)	• Provides leadership and support to the functions detailed below	• Leadership & Oversight of below	• Conducts Quality Insight visits • Chairs Enhanced Surveillance meetings i.e. Rapid Quality Reviews and Quality Improvement Groups • Deputising for execs to chair SQG and HCPE	• Leadership & Oversight of below
Head of Clinical Governance, Excellence & Patient Safety (1 x 8c) (supported by B6 Deputy Quality Manager & B4 Business Administrator)	• Contribute to JFP, FYFV, ICB strategy • Provides leadership and support to the Patient Safety Specialist in the production of the Patient Safety Strategy, Quality Strategy, System Quality Account and System Safety & Quality priorities	• Development and maintaining processes for escalation through the National Quality Board/System Quality Group framework • Review of agreed system metrics & escalation of variation	• Lead for National Quality Board escalation framework – including management of providers in Enhanced Surveillance (note 8b is lead for Standard and Elevated Quality Oversight) • Conducts Quality Insight visits	- Providing leadership, knowledge and guidance in respect of best practice in patient safety/quality practices and clinical governance and effectiveness - Identifies and leads on policy development identified from programmes such as the ICB Quality Management System, national policies, NICE and research and development.

Level	Quality Planning	Quality Control	Quality Assurance	Quality Improvement
Patient Safety Specialist (1 x 8b)	• Produce Patient Safety Strategy – including oversight of Providers' PSIRPs and PSIRF • Produce Quality Strategy • Produce System Quality Account • Develop System Safety & Quality priorities • Contribute to JFP, FYFV, planning rounds, ICB strategy • Leadership and support to Quality Leads who have oversight of specific HCIGs in their portfolios (see below)	• Support and management to Patient Safety Quality Leads (2 x 8a) – overview of all 4 HCIGs/SDUs • Review of agreed system metrics & escalation of variation	• Lead for Elevated Quality Oversight and Standard Quality Oversight processes (note, 8c is lead for Enhanced Surveillance Processes –see above) • Responsible for the production of the monthly quality report • Prep for CNO/CMO and other insight visits • Conducts quality insight visits	• Connecting ICB to national and regional patient safety fora • Providing leadership, knowledge and guidance in respect of best practice in patient safety/quality practices • System Learning forum • Lead on system Patient Safety Specialist Advisory Group to determine QI priorities (also used to escalate quality issues/risks, triangulate intelligence)
Patient Safety & Quality Leads (2 x Band 8a)	• Each Quality Lead to have oversight of 2 HCIG/SDU areas (note both Deputy Chief Nurses have oversight of 2 areas as well) • Yearly agreement of CQUINNs • Yearly agreement of contract quality schedules	• Leads on Standard Quality Oversight process – e.g. monthly one-to-one meeting with Provider Quality counterpart	• Leads on Standard Quality Oversight processes e.g. monthly meeting with contracts colleagues • Supports Patient Safety Specialist with elevated Quality Oversight • Supports writing of monthly quality report • Supports quality insight visits	• Identifies QI programmes for relevant HCIG in portfolio • Identifies system learning from incidents, and patient experience for relevant HCIG area
Patient Safety & Quality Manager (1 x Band 7)	- Carers lead - LeDeR lead	• Surveillance of quality reports from all providers • LeDeR lead	• Coordinates the writing of monthly quality report • Deputises for Quality Leads in Standard and Elevated Quality Oversight processes • Liaises with contracts team over quality issues that may need escalation	• Leads on specific system QI programmes, conferences, and events
Business Unit/Quality Team	• TBC	• TBC	• TBC	• TBC

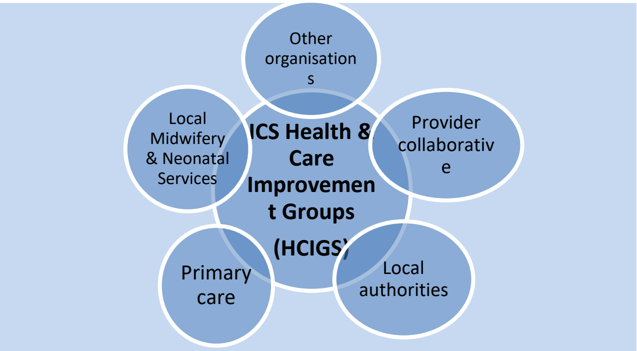
BNSSG Decision Making Framework



	BNSSG Integrated Care System Decision-Making Framework	System Function / Types of Decision	Example of Decision	System Delegation (£)
Level 0	Integrated Care Partnership Health & Wellbeing Boards (x 3)	Setting health and care strategy	Agree 5, 10, 20 year strategy	£0 - no delegated authority
Level 1	ICB Board	Oversight of NHS system financial resources Sign off of NHS LTP response / JFP Approval of operational delivery plans Sign off the outcomes framework	Approve ICS LTP response / **5-Year JFP** Approve operational plans Sign off system finance plans and ICB Budget Approve system capital priorities Approve Long Term Financial Model A decision to move outside of nationally agreed Terms and Conditions	>£1million
Level 1a	ICB Committees	Oversight and assurance for relevant functions e.g accountability for effective performance management framework	Recommend Risk Management Framework is adopted by the ICB Board	£0 - no delegated authority
Level 2	System Executive Group If Required	Actions from ICB Board Issues from ICB Committee's Oversight of major programmes Risk by exception Operational Decision making **if required**	Agree to establish a Winter Control Centre. Review recommendations from Winter Control Centre and make system operational decisions. **All decisions taken by the System Executive Group will be recorded in a register and reported to the ICB Board via the ICB Chief Executive report.**	£500K - £1million*
Level 2a	Service Delivery Unit (SDU) Transformation Hub & Intelligence Function ICB Health & Care Improvement Groups ICS Enabling Resources	Support strategic delivery across Transformation Programmes and System Financial Position	Recommend allocation of SDF funding based on understanding of population need an current services in this area	<£500K*
Level 3	NHS Statutory Organisational Boards **Provider Collaboratives **Locality Partnerships **GPCB	Set organisational strategy within the context of the health and care strategy and the Long Term Financial Model Provide oversight of organisational quality, performance and financial delivery	Approve organisational budgets within the framework of the system LTFM	£ Organisational annual budget
Level 3a	NHS Trust Executives / Divisional Boards			£ In accordance with organisations SORD

**As system matures, Provider Collaboratives, Locality Partnerships and the GPCB will be delegated budgets as system delivery partners

*ICB Executive delegated authority as set out in SORD

	BNSSG System Quality Escalation Framework	Purpose & System Function
Level 0	Integrated Care Partnership Health and wellbeing Boards (x3)	Setting Health and Care Strategy
Level 1	Integrated Care Board	Oversight of NHS Financial resources Sign off NHS LTP response/JFP. Approval of operational delivery plans Sign off the outcome's framework
Level 1a	Outcomes, Quality & Performance Committee	The quality and safety of commissioned services as set out in the annual operating plan. Improving outcomes that reduce inequalities and increase prevention. The effectiveness of patient care leading to high quality patient experience. Provider service quality performance and quality improvement initiatives. Continuous quality improvement and shared learning across the system. Assurance that statutory duties are met including Safeguarding and complaints
Level 2	Health Care Professional Executives System Quality Group	**HCPE** Forum for senior clinical, health and care professionals to support strong professional leadership. **SQG** A strategic forum to share insight & intelligence, identify opportunities for improvement, concerns/risks to quality - development of system responses to concerns/risks. HCPE and SQG will connect on joint decision making and management of system risk.
Level 2a	HCIGs Quality Improvement Group  Other organisation s Local Midwifery & Neonatal Services ICS Health & Care Improvemen t Groups (HCIGS) Provider collaborativ e Primary care Local authorities	**QIG** to support planning, coordination and facilitate the sustained delivery of actions to mitigate and address. the quality risks/ concerns within an individual provider or across the providers in the local system more generally **HCIGs** Concerns/Risks will be escalated by the • ICS HCIGS • Provider Collaboratives • Primary Care • LMNS • System Partners The NQB process will be triggered to consider the escalated concerns/risks and decisions made on required actions going forward.
Level 2b	Rapid Quality Review meeting	**RQR** Multi-stakeholder meetings set up to facilitate rapid diagnosis of quality concerns/ issues and to agree next steps, including action/improvement plans.

	BNSSG System Quality Escalation Framework	Purpose & System Function
Level 2c	Intelligence Sharing meetings (as per slides 9-15 e.g. Partner Quality Committees, system IPC group, LMNS, APMOC, Safeguarding Boards	**Intelligence sharing meeting.** An initial meeting of key stakeholders to establish the facts of the concern/risk being escalated and to agree if further formal steps are required
Level 3/3a	ICS Service Delivery Units Locality Partnerships GPCB NHT Trust/Partners divisional	Intelligence sharing/escalation (note, not exhaustive)

Level	Quality Planning	Quality Control	Quality Assurance	Quality Improvement
ICP- Roles Interpret Agree Influence Share	• Agrees annual joint forward plan and 5 year plan • Agrees joint CB strategy • Review HWB plans • Interprets national guidance	• Interprets local intelligence that indicate divergence from agreed objectives	• Review significant system audits and benchmarking • Shares patient voice material • Interpretation of high level population health data	• Shares QI best practice and significant achievements • Influence adoption of QI culture against delivery of strategic aims
ICB Board	• Strategy and transformation - Sets a vision, strategy and clear objectives for the ICB in delivering on the four core purposes of the ICS, the triple aim and the body's regulatory responsibilities; Works with Local Government partners to establish the Integrated Care Partnership encouraging a strong focus on health and care outcomes for the population. • Influences the system NHS's contribution to the wider determinants of health	• Receives updates on quality control measures of system partners and pathways through the relevant HICIGs, HCPE and OQP committee	• Receives assurance through the functions of the OQP committee and HCIGs	• Provide opportunities to promote the duty to create knowledge and innovation in health and care delivery. • Promote collaboration of system partners in QI

Level	Quality Planning	Quality Control	Quality Assurance	Quality Improvement
ICB committees (Outcomes, Quality & Performance Committee)	• Provide oversight, scrutiny and assurance of effective governance and internal control on improvement of outcomes in the population, including those that reduce inequalities and increase prevention.	• Interprets/receives local intelligence that indicate divergence from agreed objectives	• Provide oversight, scrutiny and assurance of effective governance and internal control on 1. The quality and safety of commissioned services as set out in the annual operating plan. 2. For the effectiveness of patient care leading to high quality patient experience 3. For provider service quality performance and quality improvement initiatives. • Provide assurance that statutory duties are met including Safeguarding and complaints.	• Provide oversight, scrutiny and assurance of effective governance and internal control for Continuous quality improvement and shared learning across the system.

Level	Quality Planning	Quality Control	Quality Assurance	Quality Improvement
HCIGs	• Integrated Care Strategy: Supporting the development of ICS strategic priorities (annual refresh); Brokering, defining, and mandating System Partner Agreements to facilitate the delivery of the objectives defined by the System Executive Group • Joint Forward Plan (JFP): Supporting the development of the JFP (annual refresh); Accountable body for the delivery of the JFP objectives defined by the System Executive Group • ICS Green Plan: Actively contribute to the delivery of the ICS Green Plan by developing solutions which deliver measurable benefits to the sustainability agenda and the net zero target.	• ICS Operational Delivery: Overseeing operational activity of ODGs; receiving regular Highlight Reports, acting on recommendations and managing any escalated risks • Financial/Budgetary Oversight; Receive financial reports and information relevant to the domain of the HCIG. • ICS Risk Management: Monitoring and actively managing ICS risks (controls, mitigations and actions) of not achieving the HCIG defined objectives, and those escalated by the relevant ODGs and Working Groups in accordance with the ICB Risk-Management Policy; Escalating ICS Risks to the System Executive Group in accordance with the ICB Risk-Management Policy; Work collaboratively with the System Quality Group to ensure risks to the quality of services are appropriately managed in accordance with National Quality Group Guidance.	• ICS Oversight: Receiving reports by exception from ICS Oversight Groups when required; Commissioning data dashboards to monitor progress and measure the impact of activity that achieves their defined objectives; Ensuring actions from the ICB Board and the System Executive Group are being actively progressed as directed; Where the delivery of a defined objective is influenced by the activity of another HCIG, work collaboratively with that HCIG to reach a joint consensus, escalating to the System Executive Group by exception.	• Transformational Improvements: Commissioning the Transformation Hub when Transformational Improvements are required to achieve the HCIG defined objectives; Act as Gatekeeper for the Transformation Hub when Transformational Improvements have been commissioned by the HCIG. • Continuous Improvements: Commissioning improvement activity via the appropriate ODG, supported by the ICBs Service Delivery Units, to achieve the HCIGs defined objectives. This may involve standing up a (time limited) Working Group to deliver specific improvements.

NHS

Bristol, North Somerset
and South Gloucestershire
Integrated Care Board

Learning and Development Policy

Please complete the table below: *To be added by corporate team once policy approved and before placing on website*	
Policy ref no:	47
Responsible Executive Director:	[redacted], Chief People Officer
Author and Job Title:	[redacted], Project Manager – Talent and Learning
Date Approved:	6 November 2023
Approved by:	[redacted], CEO
Date of next review:	November 2026

Policy Review Checklist

	Yes/No/NA	**Supporting information**
Has an Equality Impact Assessment Screening been completed?	Yes	See Appendix B
Has the review taken account of latest Guidance/Legislation?	Yes	Apprenticeships Core Skills Training Framework NHS People Plan
Has legal advice been sought?	NA	
Has HR been consulted?	Yes	Written in consultation with HR and based on other ICB Appraisal Policies
Have training issues been addressed?	Yes	Education and Awareness of processes by which training may be accessed already

	Yes/No/NA	Supporting information
		promulgated. On policy adoption and launch, to be announced on stand-up and in The Voice and on The Hub
Are there other HR related issues that need to be considered?	No	
Has the policy been reviewed by Staff Partnership Forum?	No	To be presented on 23 August
Are there financial issues and have they been addressed?	NA	Pressure on L&D Budget. Process now in place to manage any spend
What engagement has there been with patients/members of the public in preparing this policy?	NA	Internal staff only
Are there linked policies and procedures?		Appraisal Policy
Has the lead Executive Director approved the policy?	No	CPRG 9 Aug
Which Committees have assured the policy?		CPRG 9 Aug, SPF 23 Aug
Has an implementation plan been provided?	Yes	Internal processes for managing various forms of learning – so Apprenticeships, CPD, Individual & Collective training have already been put in place, tested, and are now in use
How will the policy be shared with: • Staff • Patients • Public		Announcement in The Voice and on The Hub. Documents are available through The Hub, ConsultOD and ConsultHR No requirement for public consultation / awareness

	Yes/No/NA	Supporting information
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	No	Measured using the LDP to review costed applications
Has a DPIA been considered in regards to this policy?	Yes	Via CRPG IG attendance
Have Data Protection implications have been considered?	NA	

Table of Contents

Appendix A – Outline of Content - Justification for Collective / Team Training

Appendix B – Equality Impact Assessment

ICB Learning and Development

1 Introduction

Effective Learning & Development (L&D) supports sustainable business success in the rapidly changing external environment of the ICB. Rapid learning, adapting to new challenges, and embracing innovation are vital for our continued success. We prioritise the development of individuals, teams, and groups, allowing employees to enhance their skills and knowledge, enabling the organisation to meet current and future business needs. We must apply our Core Values to strengthen interactions within the ICB and with stakeholders, customers, and care communities.

1.1 BNSSG ICB Values

This policy aligns with the core values of the ICB, which include supporting one another, embracing diversity, collaborating effectively, and striving for excellence. By implementing a robust L&D system, we not only align the organisation with the standards set by our governing bodies, but we also ensure that every individual across the organisation is afforded adequate learning opportunities to pursue growth and chase excellence across the time course of their careers. Moreover, this policy contributes to the overall ICB People Plan. L&D offers enhance individuals' capabilities in their current roles through skill building, brainstorming, and the fostering of new perspectives. Effective L&D enables us as an organisation to support each other in achieving both our organisational and individual goals.

2 Purpose and scope

This policy establishes frameworks, processes, and guidance for effective Learning & Development (L&D) by enabling managers and staff to utilise available learning resources. It outlines managers' responsibilities in providing initial induction and ongoing support to ensure staff have the necessary knowledge, skills, and permissions to contribute to ICB Goals. The policy also addresses monitoring and controlling the training budget to maximise return on investment.

Equality of access to learning support is emphasised, ensuring all ICB members' learning needs and objectives are acknowledged, considered, and evaluated within the available budget. The policy applies to all permanent, fixed-term, full-time, part-time employees, and secondees of the ICB, excluding contractors or consultants, except for Corporate and Local Induction and ensuring safety and relevant training for temporary ICB workforce members.

3 General Principles

Employee Support: BNSSG ICB prioritises equipping employees with the necessary knowledge and skills for successful performance. Induction and orientation programs led by line managers provide clarity and support for new staff.

Identification of Learning Needs: Regular analysis through the Appraisal Policy identifies learning needs. Personal Development Plans (PDPs) should prioritise activities to address operational challenges and achieve ICB objectives.

Provision of L&D Support: L&D support includes diverse activities beyond formal training. Line managers are encouraged to be creative when planning interventions.

Fair & Equitable Application: This policy identifies development needs clearly and provides appropriate responses. It fosters a learning delivery system which is fair to all while being efficient and considering resource constraints.

Adoption of a Systems Approach to L&D Provision

The ICB adopts a systematic approach to L&D provision involving the following activities:

- Induction and orientation for staff in new roles.
- Identification, clarification, and agreement of learning needs.
- Design, development, and delivery of planned interventions.
- Validation of interventions to ensure effectiveness and understanding of constraints in applying learning.
- Evaluation of learning to measure its impact on performance and contribution,
- Sharing of learning across teams and the organisation, maximising the value of individual learning.

This approach ensures maximum value from resource investments in learning interventions, specifically by:

- Providing proportionate training based on identified needs.
- Delivering cost-effective and quality training.
- Ensuring the appropriateness of interventions to meet expressed needs.
- Supporting the adoption and utilisation of new skills and knowledge.
- Considering equality, diversity, and inclusion in planning interventions.
- Offering equal access to learning opportunities while managing the limited budget effectively.

4 L&D Activities covered by these Policy Provisions

Local & Corporate Induction

Local & Corporate Induction: Induction serves as an opportunity for the ICB to welcome new staff, ensuring they have the necessary knowledge and support for their roles. It dramatically influences their integration, job satisfaction, and perception of the organisation’s brand and values. Onboarding further familiarises new staff with their team and locality and provides tools for them to become valued team members quickly. Effective onboarding positively impacts employee satisfaction, engagement, and tenure.

Critical outcomes of local induction include developing good work habits aligned with safety and environmental practices, making new staff feel valued and part of the team, and ensuring understanding and appreciation of the ICB's working culture and core values. Line managers are responsible for providing appropriate local induction, which may vary between teams and locations. Guidance and suggested content can be found here on ConsultHR.

Onboarding may commence before the new staff member's start date, establishing early communication and sharing relevant information and is the responsibility of the line manager. Corporate Induction, to which many departments make contributions, is the responsibility of the Office of the Chair and Chief Executive. All new staff must attend Corporate Induction, facilitated by line managers, ensuring availability. Temporary staff, contractors, and consultants must also participate in Corporate Induction and receive limited local induction, particularly on Health & Safety and safe working practices in their respective areas.

Statutory & Mandatory Training

Statutory and mandatory training are training opportunities required for all or some portion of staff directed by national government organisations, local authorities, the ICB, and/or individual directorates (in the case of role/team specific training needs). It ensures compliance with legislative duties and is essential for running a safe and effective service. For instance, the ICB is responsible for providing core health and safety awareness training to all new employees; failure to meet this can result in penalties.. Periodic updates are necessary to maintain compliance, and the People Directorate manages the scheduling of refresher or requalification training as required.

The People Directorate generates regular reports to the Executive, demonstrating compliance rates. Non-compliance levels that may impact the ICB's ability to deliver services effectively and safely to the community are identified and addressed.

Individual Learning

Individual learning refers to short-term learning activities undertaken by staff members to address their specific learning needs and acquire new skills and knowledge. This learning serves the following purposes:

- Building competency and expertise in their current role.
- Adapting to role enhancements resulting from job expansion or changes driven by technology or other factors.
- Preparing for a designated new role within BNSSG.

These learning needs are typically identified through regular conversations between line managers and staff members, such as 1:1 meetings or appraisals. The individual's Personal Development Plan (PDP) should clearly define the needs.

Line managers are encouraged to think creatively about suitable learning interventions, considering resource utilisation and financial costs to the ICB. If the solution does not incur direct economic costs, managers can integrate the learning activities into the staff members' day-to-day responsibilities without formal permission.

If the learning solution does incur financial costs, the individual must formally apply for funding. The process for funding applications is outlined in the L&D Application Process available on ConsultOD. Before providing local budget support, directors must consider whether the proposed support aligns with the Learning & Development Panel's (LDP) responsibilities and its operating principles. The L&D Application Process details the steps and requirements for funding requests.

Continuing Professional Development (CPD)

Continuing Professional Development (CPD) refers to the process undertaken by individuals to enhance their skills, knowledge, and experiences throughout their careers. It involves tracking and documenting the development activities individuals need or desire to pursue formally and informally to achieve their career aspirations and personal/professional growth. Many of these activities will be longer, more in-depth endeavours than individual learning and may or may not result in credentialing opportunities.

At all levels within the ICB, staff members are encouraged to create a personal CPD Plan to identify potential future career, professional, and individual growth pathways aligned with their aspirations. CPD activities encompass various methodologies such as workshops, conferences, e-learning programs, best practice techniques, and idea sharing, all aimed at providing individuals with effective development opportunities.

While the ICB supports individuals engaging in CPD activities, this support is contingent upon the activities not hindering their ability to perform their job effectively. Line managers and directors are responsible for ensuring that supporting CPD activities is sufficient for the team, group, or directorate to fulfil operational outcomes and strategic imperatives.

When possible and practical, directors can and may support CPD activities through appropriate use of local resources. In cases where staff members seek financial support from the ICB's central L&D budget, a formal application must be made. This application may include requests for course/event fees, subsidies/refunds for accommodation, subsistence, travel costs, time off during working hours for attendance or study, or a combination. The CPD Application process, available on ConsultOD, provides guidance and the appropriate application form.

Requests for CPD support will be reviewed, considering the availability of funds. Priority will be given to requests for support for individual learning.

While the ICB considers supporting staff on temporary or fixed-term contracts, the investment return will be evaluated based on the likelihood of staff members leaving at the end of their contracts.

Team or Collective Learning

Team or collective training within the ICB can be categorised into two activity levels.

The first level involves the ICB identifying performance issues requiring teams or staff groups to undergo collective training. This training aims to address those issues and enhance the overall competence of the organisation. For example, if the management population needs additional skills or knowledge in a particular subject, they would be enrolled in relevant courses or events organised at the corporate level. The Talent and Learning Manager (T&LM) is responsible for managing these events and ensuring the attendance of the identified personnel.

The second activity level pertains to individual managers recognising the need for team-based skills or knowledge development. In this case, if internal resources or local (directorate) budgets can fulfil the training requirements, involvement of the T&LM is not necessary, except for advice and guidance. However, if the team or collective learning requires funding from the L&D budget, the line manager must present a case justifying the need for ICB support. The justification should address relevant issues outlined in Appendix B of the policy and be concise, usually at most two pages.

Line managers are advised to consult with the T&LM before finalising any solution that incurs financial costs to ensure that similar training needs have yet to be previously addressed within the ICB and to receive guidance on assessing business needs and the likelihood of the case being accepted by the LDP.

Work Experience

The ICB recognises the value of offering work experience (WE) placements to young individuals from a diverse range of communities. These placements allow young people to gain work experience and develop essential skills to enhance their future employment prospects. The ICB views WE as a positive engagement strategy and identifies several benefits, including recruitment opportunities, fresh perspectives, talent development through apprenticeships, challenging perceptions of young people's skills, and staff development through mentoring roles.

Under the Work Experience Placement Programme (WEPP), young individuals can volunteer for one to two weeks. They will be matched with suitable host managers who will provide day-to-day supervision. The T&LM oversees the program and manages all WE placements. Each year, the T&LM presents the WEPP to the L&D Panel, outlining collaboration with schools, program timelines, school visits, marketing efforts, application and selection processes, induction, placement plans, and end-of-placement activities.

All participants in the WEPP receive an ICB induction that covers essential aspects of health and safety, building familiarisation, contact information, and specific instructions related to their placement. For more information about the ICB WEPP, individuals can contact the T&LM, which is responsible for program development.

5 Duties & Responsibilities

a. Staff Members

Learning and development are most effective when the individual takes responsibility for identifying opportunities for self-development which will enhance their work performance by acquiring new skills and knowledge. This includes:

- Taking an active role in planning their personal development and undertaking agreed development activities.
- Sharing their learning and experiences with others within the ICB and assisting with evaluating the effectiveness of all learning interventions.
- Individuals are expected to complete their statutory and mandatory training and remain compliant with the need to do so within identified timescales.
- Learning needs and opportunities will be identified with their line manager during informal 1-1 conversations and in their annual appraisal meeting. These need documenting by the Appraisal Policy. This will generate an agreed Personal Development Plan (PDP) for the individual.

b. Line Managers

Line Managers are responsible for:

- Delivering local induction for personnel employed within their team and defined work areas.
- Orientation sessions for all staff.
- Clear direction on local health and safety issues.
- Ensuring compliance with all ICB policies and procedures.
- Local Induction requirements are identified in the guidance on Induction and Onboarding, which can be found on the Hub and via the ConsultHR site. They will support staff members in identifying learning needs, ensuring that they review these with staff regularly through 1-1 discussions and engagement with the appraisal process.
- Ensure that Appraisal PDPs are completed and then regularly updated through 1-1 conversations and six-month appraisal reviews.
- Encourage and facilitate their team members' involvement in learning and development activities and providing guidance/feedback regarding the skills and knowledge required for their current role.
- Balance the competing demands of staff wishing to access learning opportunities with the operational outputs required of their team.

- Think critically to determine whether a request for ICB support is feasible and supportable and should not simply rubber-stamp a request but take an even-handed and objective approach to determine whether it can be supported at the local management level.
- Monitor and evaluate the effectiveness of any learning intervention their staff may undertake. Support can be obtained from the T&LM. Ensure that staff members implement the skills they have gained through training and that any feedback on the impact of that training is shared within their teams and across the wider ICB as appropriate.
- Report to the T&LM when clawback provisions must be initiated upon a staff member's departure from the ICB.

c. Executive & Senior Management Teams

- Actively encouraging training and development across their directorate, group, or department to ensure they can enable the ICB to meet its strategic goals and operational objectives.
- Consider applications for learning and development support, with due regard to their directorate's ability to deliver fully against their strategic priorities and current objectives and to best shape directorate resources, both capacity and capability to meet future demands that might be placed upon them.
- Engage with Learning and Development Panel (LDP), which is described below, which will determine how the limited L&D budget is best shared fairly and equitably to meet the learning needs of the business.

d. Talent and Learning Manager (T&LM)

- The T&LM is responsible to the Chief People Office Business Partner for the efficient and effective delivery and management of the following L&D products and services:
- Undertaking L&D planning to support Organisation Development initiatives.
- Establishing a range of methods (internal and external to the ICB) to facilitate/deliver learning and development interventions.
- Supporting managers as they draw up their individual and team development plans.
- Procuring/providing internal and external L&D support, including sourcing and booking formal training events, providing external training capability when necessary, and staff enrolment on external programmes and courses.
- Administering the Learning & Development Panel, ensuring that all applications for support for learning interventions are seen and evaluated by that panel in a timely fashion.
- Designing and delivering internal management, leadership, and other business-related development programmes.

- Monitoring, validating and subsequently evaluating learning and development activities conducted across ICB, including the continuous improvement of long-term programmes.
- Establishing a strong relationship with ConsultOD staff to optimise the platform and associated resources.
- Supporting line managers in ensuring that staff complete Statutory and Mandatory training as required and directed by the Executive Team. Providing regular reports on compliance as necessary to comply with current regulations and legislation.
- Ensure staff members that utilise ICB L&D funds understand the clawback provisions relating to their funding application and advise line managers and staff in the implementation of these provisions.

e. The Learning & Development Panel (LDP)

The LDP comprises members of the Executive Team and housed within the Vacancy Control Panel, which meets weekly and is chaired by the ICB CPO Business Partner. The LDP occurs as needed when applications are submitted for consideration. The panel has no quorate; all executive team members are invited to attend. The T&LM will staff all papers to the Executive Team and will be responsible for all administration about the work and outputs of the LDP. This LDP will determine whether individual applications are approved for support and how that support is allocated per the two principles established below. One is to ensure equality of access to learning opportunities across the ICB. This creates an equitable approach that ensures all within the ICB do get the opportunity to apply for funding and that available funds are spread, as far as possible, fairly and evenly across the ICB.

Second, to ensure that funds to pay for learning and development solutions, where those solutions are liable to be funded from the L&D Budget, are correctly identified and directed. Priority for spend is to address issues of current performance, then to prepare individuals to take on enhancements to their current role and to prepare them for the next, clearly identified role. After that, and where limited funds permit, support individuals who wish to access CPD opportunities and gain ICB support to enable them to do so. The LDP will determine whether it is in the interests of the ICB to support applicants for Apprenticeships to be funded from the ICB Apprenticeship Levy. This will be determined by the volume of requests for financial support and the need to process specific requests in line with admission dates, etc., set by external providers.

The LDP will decide whether the ICB will support such requests based on information provided by the T&LM. This will cover, amongst other issues:

- How much L&D Budget remains unspent at the time of review?
- How much support has already been given to specific programmes or courses? This will range from attendance on NHS Leadership Academy

Programmes to our need to meet our corporate responsibilities for providing certain services across the ICB (e.g., the provision of First Aid-trained staff).

- Another known/forecasted spending against budget to meet any statutory, regulatory, or other mandated training as directed by the CEO.
- Planned collective learning activities determined at ICB Level.
- Where significant spend has already been allocated in some operational areas.
- Where requests have greater priority over others due to the nature of the business case identified – where that case identifies business-critical skills or knowledge shortages, or where the return on the investment into that learning is significant.
- Where support for specific requests will allow the ICB to satisfy its need to meet diversity and inclusion criteria, the Outcomes from those LDP deliberations will be made known to individual applicants by the T&LM, who will manage all subsequent actions pertinent to that request with due regard to the LDP decision. Dates for forthcoming LDPs and closing dates for applications to be considered at those LDPs will be communicated regularly across the ICB.

6 Applying for Funding or Financial Support for L&D Activities

The BNSSG ICB Appraisal Policy is designed to create clear outcomes from the conversation between the line manager and the staff member being appraised. One of those clear outcomes is a PDP intended to capture all learning needs of the individual concerned. The PDP must be agreed upon between the line manager and staff member (and signed off as such) before any subsequent actions regarding learning support can be undertaken. That PDP may contain a mix of development needs. Those that can be satisfied through learning interventions where there is no financial support to be provided by the L&D

The budget should be progressed by line managers/directors as per the appropriate headers under section 4 of this policy:

- Individual Learning
- Continuing Professional Development
- Team and Collective Training.

Where the need requires support from the L&D Budget, the priority for budget support must be evident. It is to satisfy current, known needs for the employee’s current role. Then it needs to be identified for any enhancement to that current role or in preparation for the next recognised role. Only when those needs have been adequately addressed will the LDP consider applications for financial support to undertake CPD activities. Apprenticeships are different because we have an Apprenticeship Levy to spend on learning opportunities, where the monies within that levy account are ring-fenced. However, this levy is not substantial, so the L&D Panel will also undertake the same controls and evaluation of any application. The detailed process by which an individual may apply for ICB financial support for learning and development activities may be found here on ConsultOD. The applicant should log onto their personal ConsultOD account and follow the simple guides that can be found on the Home Page. All application guidance, simple process maps, application forms, and other helpful advice and information may all be seen the same way. Inevitably, some staff members will be left disappointed at decisions reached by the LDP. The T&LM will be available to discuss alternatives to requests that do not get final approval, and where an applicant does not gain approval for a CPD event or activity, they may apply again (subject to continuing support from their line manager and director) in the next financial year when further funds may be available within the budget.

7 Training Budget – Control & Use

The People Directorate holds the Central Learning & Development Budget. The ICB CPO Business Partner is the official Budget Holder. The final authority for spending lies with the Chief People Officer (CPO). Responsibility for recording expenditures, reporting on current and forecast spending, and providing regular reports on that expenditure lies with the T&LM. The CPO will direct what reporting structures need to be in place and the frequency of that reporting. The T&LM will collate all requests for learning support – regardless of their origin or purpose - where such requests, once approved, will create expenditure from the L&D Budget. The T&LM is responsible for updating all centrally held learning records and ensuring that those records are available and offered up for review as required. Directorates each have a smaller budget to provide funds for directorate-level events such as away days, conferences, etc. Using these budgets is out of the scope of the LDP decision-making process. To ensure equitable support to staff, these directorate budgets should not be used to fund staff members seeking financial support from the ICB for individual training events or CPD activities. Individuals who wish to request such support must do so by completing the application process. Line managers ensure all staff members follow the correct application process.

8 Clawback Provisions

The ICB are committed to supporting staff who wish to further or better their professional or career development by undertaking CPD activities. Where staff members request financial support from the ICB to do so, the cost to the ICB can mount quickly when a combination of course fees, reimbursement of expenses, and work time allowed for attendance on CPD activities or for private study, examinations, etc., is requested. It is reasonable for the ICB to wish to achieve a return on its investment in that staff member before they choose to move on and leave the ICB. Equally, where a staff member is granted financial support and then fails to attend or complete the activity for which support is given, it would be reasonable for the ICB to look to recoup some of the monies that had been paid to the staff member for the specific reason of attending that activity. It follows that should a staff member fail a final exam or assessment, where the successful completion of that CPD activity would be through that examination, assessment, or similar, again, it would be reasonable for the ICB to look to recoup monies paid to support that CPD activity. This is popularly referred to as claw back. Where the ICB would intend to recoup costs in those circumstances, it will clearly define the intention and details of the claw back scale in a written agreement between the ICB and the staff member would effectively constitute a contract between both parties. This “Learning Contract Letter” will identify the specific costs that can be deducted from any salary or other payments due to the staff member. The amount the ICB would claw back in the event of any lack of performance identified above would be proportionate to the amount the ICB had lost due to that lack of performance. It is a genuine estimate of the loss to the ICB, as the opportunity afforded to one individual cannot be afforded to another. Where the ICB institutes a claw back agreement, it will ensure that the agreement is proportionate to the loss the ICB has suffered. It will also recognise where there has been a return in part on the original investment. ICB claw back provisions are:

1. Where a staff member leaves the employ of the ICB before finishing their CPD activity
    a. All costs incurred relevant to that activity, including any course or programme fees, expenses already reimbursed, exam fees, etc.
    b. A maximum sum equal to the net salary costs per hour of work time to support completing that CPD activity.
2. Failing to attend at least 75% of stipulated activities resulting in non-achievement of the intended benefit:
    a. All costs incurred relevant to the activity as per point 1a above.
    b. A maximum sum equal to the net salary costs per hour of work time to support completing that CPD activity. There may be occasions where attendance is affected by ill health. In such circumstances, the CPO will determine the funds to be recouped.
3. Leaving the ICB within the following periods after completion of that CPD

1. Activity:
    a. Within 12 months — reimbursement of 100% of all costs incurred.
    b. Within 18 months — reimbursement of 50% of all costs incurred.
    c. Within 24 months — reimbursement of 25% of all costs incurred.

The ICB will consider whether a staff member leaving the ICB to undertake a role in the wider system of care should be absolved from the requirement to pay back monies under the terms of these ICB claw back provisions. This will be agreed on a case-by-case basis by the CPO. The ICB reserves the right to vary the abovementioned terms, and the CPO will agree upon any variation.

9 Equality Impact Assessment

The ICB is committed to ensuring equality of learning opportunities; hence no staff member will be excluded from learning on the grounds of gender (including gender reassignment), marital status, family status, religious belief, disability, age, race, ethnicity or nationality, sexual orientation, or where they possess other protected characteristics under the terms of the Equality Act 2010. Part-time and fixed-term staff members will have equal access to learning and development opportunities appropriate to their roles. Please refer to BNSSG ICB's Equal Opportunities and Dignity at Work policies for further information. It is the responsibility of the T&LM to maintain the visibility of spend on learning activities and interventions across the ICB and report any inconsistencies with this policy element to the CPO. If any ICB employee believes that they or a colleague have been disadvantaged by anything contained in this policy, they should, in the first instance, contact the T&LM, who will then actively respond to the enquiry. The Equality Impact Assessment for this policy is in Appendix B.

10 Training requirements

Support will be provided to all Line Managers in implementing and applying this policy. The first point of support will be with the T&LM, who is available to provide advice and guidance on all aspects of this policy to managers and staff members alike.

11 Monitoring Compliance & Effectiveness

This policy will be reviewed in July 2024 to assess the provisions' effectiveness and currency. After that, it will be reviewed every two years or when the CPO deems it prudent to do so. Financial and other data will be collected and reported by the T&LM to the CPO

12 Countering Fraud, Bribery, and Corruption

The ICB is committed to reducing and preventing fraud, bribery and corruption in the NHS and ensuring that funds stolen by these means are put back into patient care. During the development of this policy document, we have given consideration to how fraud, bribery or corruption may occur in this area. We have ensured that our processes will assist in preventing, detecting and deterring fraud, bribery and corruption and considered what our responses to allegation of incidents of any such acts would be.

In the event that fraud, bribery or corruption is reasonably suspected, and in accordance with the Local Counter Fraud, Bribery and Corruption Policy, the Team will refer the matter to the ICB's Local Counter Fraud Specialist for investigation and reserve the right to prosecute where fraud, bribery or corruption is suspected to have taken place. In cases involving any type of loss (financial or other), the ICB will take action to recover those losses by working with law enforcement agencies and investigators in both criminal and/or civil courts. .

13 References, Acknowledgements & Associated Documents

Appraisal Policy

Guidance documentation application forms are stored here on Consult OD.

14 Appendices

Appendix A – Outline of Content - Justification for Collective / Team Training

Your justification for ICB financial support for the implementation of a learning and development solution should be clear, concise, and to the point. As a guide, it should take no more than two sides of A4 paper to convey.

Your case should stand on its own, be easy to read and understand, and offer a clear understanding of the value in adoption.

You may present it in a local team or directorate format, but it should fully cover all the points listed below.

BEST PRACTICE CONTENT FOR TRAINING JUSTIFICATION

1. Define the problem / challenge / opportunity in clear and concise terms, no more than two to three sentences contained in the opening paragraph. Do not simply state that training or other learning activity is required.

2. Describe the situation / context in which the above problem / challenge / opportunity is set.

3. Describe the potential costs, consequences, and losses that the ICB may suffer, should the issue at step 1 above not be addressed or exploited. These may not be financial and so some lateral thinking may be necessary here to articulate these issues – so staff morale, staff engagement, retention of key personnel, etc., are all valid consequences. If you are able to place a monetary value on your points here, it will strengthen your case.

4. State clearly the various options you have identified that would address the problem or challenge or allow the positive development of the opportunity. If possible, ensure that you clearly state the total cost of implementing any of the other solutions.

5. Describe the preferred solution and offer some analysis as to why you recommend that solution. If the solution is multi-faceted or complex, describe the key features of the whole solution that require support from a learning and development perspective. Again, ensure you include total costs of adopting that particular solution.

6. Describe the key benefits that the ICB will accrue from adopting the preferred solution.

7. Create a summary paragraph to capture all salient points in condensed form – so issue, consequence, recommendation, and benefits.

8. State clearly the actions you would wish the ICB to adopt or to give permission for, and timescales for implementation.

Appendix B – Equality Impact Assessment

Equality Impact Assessment Screening		
Query	**Response**	
What is the aim of the document?	Provide advice and guidance on Learning and Development	
Who is the target audience of the document (which staff groups)?	All staff groups.	
Who is it likely to impact on and how?	Staff	Support staff in engaging with L&D Learning and Development opportunities.
	Patients	No
	Visitors	No
	Carers	No
	Other – governors, volunteers, etc.	No
Does the document affect one group more or less favourably than another based on the 'protected characteristics' in the Equality Act 2010:	Age (younger and older people)	No
	Disability (includes physical and sensory impairments, learning disabilities, mental health)	Yes – staff with visual impairment will need additional support with completion of forms and audio description where needed. Staff with hearing impairment may need visual representation. The performance of staff with learning disabilities, long term and health conditions and neurodiversity may be affected by their conditions and adjust may be required including in the preparation of associated paperwork. Staff with mental health issues may also find the process daunting and require additional support.
	Gender (men or women)	Yes – female employees are statistically more likely to be in part time roles in the organisation so are more likely to miss opportunities for development – managers must be flexible around such working arrangements.
	Pregnancy and maternity	Yes – staff on Maternity or Adoption leave will miss training opportunities. Managers need to ensure staff on such leave are kept reasonably well informed and updated on organisation developments.

	Race (includes ethnicity as well as gypsy travelers)	No
	Sexual Orientation (lesbian, gay and bisexual people)	No
	Transgender people	No
	Groups at risk of stigma or social exclusion (e.g., offenders, homeless people)	No
	Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)	No

Healthier Together
Improving health and care in Bristol,
North Somerset and South Gloucestershire

NHS
Bristol, North Somerset
and South Gloucestershire
Integrated Care Board

Acceptable Use of IT Policy

Complete the blank cells in the table below. The rest will be added by the corporate team once the policy approved and before it is added to the website.	
Policy ref no:	48
Responsible Executive Director:	[redacted], Chief Transformation and Digital Officer
Author and Job Title:	[redacted], Head of Digital ICB [redacted], Information Consultant, SCW CSU
Date Approved:	19th December 2025
Approved by:	[redacted], Chief Executive
Date of next review:	September 2027

Policy Review Checklist

	Yes/No/NA	Supporting information
Has an Equality Impact Assessment Screening been completed?	Yes	Appendix A
Has the review taken account of latest Guidance/Legislation?	Yes	
Has legal advice been sought?	No	Based on South Central and West Commissioning Support Unit (SCW CSU) Acceptable Use Policy version 5.0 and BNSSG AUP for N365 Policy
Has HR been consulted?	Yes	As part of the Corporate Policy Review Group
Have training issues been addressed?	Yes	Support is available via the IT Helpdesk (Top desk)
Are there other HR related issues that need to be considered?	Yes	Links to Disciplinary Policy
Has the policy been reviewed by Staff Partnership Forum?	No	Not required
Are there financial issues and have they been addressed?	Yes	This policy covers the use of IT equipment which is funded through existing budgets
What engagement has there been with patients/members of the public in preparing this policy?	N/A	
Are there linked policies and procedures?	Yes	The policy is one of a suite of IG/IT related document which support the ICB's responsibilities listed in the Data Security and Protection Toolkit (DSPT)
Has the lead Executive Director approved the policy?	Yes	Via the ICBs Information Governance Group
Which Committees have assured the policy?	Yes	ICBs Information Governance Group
Has an implementation plan been provided?	Yes	See Implementation Plan
How will the policy be shared with staff?		Via Consult OD and the intranet, refer to the Implementation Plan

	Yes/No/NA	Supporting information
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	Yes	Via Consult OD – annual mandatory requirement
Has a DPIA been considered in regards to this policy?	Yes	Not required
Have Data Protection implications have been considered?	Yes	This Policy addresses all necessary information governance requirements

Version	Date	Consultation
1.0	27/2/2024	Cosmetic changes, changes from CCG to ICB and alignment to SCW Acceptable Use Policy
1.1	30/1/2025	Review of Policy to make more user friendly
1.2	10/02/2025	Add in N365 components for Acceptable Use – separate Policy is being written Amendment to Section 13 (incorporating what was originally stated in a separate section 16 entitled electronic mail and instant messaging Changes to state you must never share your password
1.3	10/04/2025	Updated to include N365 & AI. This will enable the recently agreed N365 policy (referenced above) to be removed from circulation.
1.4	01/11/2025	Incorporate comments from CPRG and take out any duplicated statement from amalgamation with N365 Policy.

Table of contents

Acceptable Use of IT Policy

1 Introduction

This document sets out Bristol, North Somerset, and South Gloucestershire Integrated Care Board (BNSSG ICB) Policy for the Acceptable Use of Information Technology, electronic systems, and equipment to ensure they are used in a secure, lawful and responsible manner.

It forms part of BNSSGs Information Security Management System. A suite of related policies which support the Data Security and Protection Toolkit (DSPT).

1.1 The Information Security Management System (ISMS)

The objective of the ISMS is to define a coherent set of policies, standards, and architectures that:

- sets out the governance of IT security.
- provides high level policy statements on the requirements for managing IT security.
- defines the roles and responsibilities for implementing the IT security policy.
- identifies key standards, processes, and procedures to support the policy.
- defines security architectures that encapsulate the policy and support the delivery of secure IT services.

There are several policies which comprise the ISMS which include the following:

Password Policy; Network Security Policy; IT Disposal Policy; Anti-Virus Policy and Information Security Policy.

The South Central and West Commissioning Support Unit's (SCW CSU) IT estate is governed by certain policies IT Policies - Self-Service Portal that have been approved by BNSSG. Additionally, the ICB has its own technical policies for systems run under their tenant management.

The Acceptable Use Policy (AUP), Secure Data Environment (SDE) standards, IT policies, Artificial Intelligence (AI) governance, Information Governance (IG), and Microsoft 365 (N365) controls are interconnected components of a comprehensive digital strategy. Each exists to address distinct but overlapping risks and responsibilities: AUP defines user behaviour expectations; SDE ensures technical safeguards for secure operations; IT policies set overarching rules for technology management; AI governance addresses ethical and compliant use of intelligent systems; IG ensures data protection and regulatory compliance; and N365 provides platform-specific security and collaboration controls. Together, they create a layered approach that mitigates risk, supports legal and regulatory obligations, and enables safe innovation. The reason for multiple policies is that no single document can cover all dimensions—technology, people, processes, and platforms—without losing clarity or enforceability.

1.2 BNSSG ICB Values

This policy supports the ICBs activities by ensuring they are secure and compliant therefore ensuing that we are acting with integrity and are doing the right thing.

2 Purpose and scope

2.1 Purpose

This policy offers a high-level structure within which all staff (users) are required to carry out their daily tasks. The Policy defines the principles and minimum controls expected to protect the ICBs IT as well as its information and data.

This policy aims to ensure the secure and appropriate use of all IT, systems and applications, preserving the confidentiality, integrity and availability of its information and protecting personal data, ICB business data, and the integrity of its IT systems/apps.

All users are responsible for understanding and complying with this policy.

This policy provides clarity on the appropriate, safe, and legal way in which users can make use of IT equipment, services, and systems/apps by:

- Clarifying acceptable and unacceptable use of all ICB systems/apps, networks, and IT equipment.
- Ensuring the ICB legal and statutory requirements are met.
- Protecting the organisation against potential liability.
- Minimise risk of inadvertent, accidental, or deliberate unauthorised access or disclosure.
- Reduce or avoid security threats by increasing awareness, communication and disseminating good practice.
- Control the copying/distribution of copyrighted materials.

2.2 Scope

The ICB's expectations for user behaviour with and through its digital capacity are set out in this policy, together with the mandatory measures that must be adhered to secure BNSSG's information during its lifecycle.

It is applicable to the use of all IT equipment, services and systems/apps utilised by users. This includes but is not limited to, the functionality introduced as part of the N365 suite of applications and any Artificial Intelligence (AI) tools, features, or integrations without other systems/apps.

This policy applies to any individual authorised to undertake work on behalf of the ICB, and who have been provided with access to IT equipment and systems/apps.

This includes:

- permanent or temporary staff, contractors, and agency staff.
- any third-party accessing ICB IT systems including volunteers and students.

- all those engaged in duties for the ICB, under a letter of authority/honorary contract or work experience.

The term user is used throughout this policy to encompass the above.

3 Duties – legal framework for this policy

The legal framework on which this acceptable use policy and other related information security policies are based is as follows:

- UK General Data Protection Regulation 2016/679 (UK GDPR)
- Data Protection Act (DPA) 2018
- Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws, implementing them as amended from time to time.

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality and the processing and sharing of personal data including:

- Human Rights Act 1998
- Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015
- Common Law Duty of Confidentiality
- Privacy and Electronic Communications (EC Directive) Regulations
- The Security of Network & Information Systems Regulation (NIS Regulations) 2018
- Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse)
- Copyright, Designs and Patents Act 1998
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health Records Act 1990
- Fraud Act 2006
- Criminal Justice and Immigration Act 2008
- Equality Act 2010
- Terrorism Act 2006
- Malicious Communications Act 1988
- Digital Economy Act 2010 and 2017
- Counterterrorism and Security Act 2015

- Bribery Act 2010
- Economic Crime & Corporate Transparency Act 2023

4 Responsibilities and Accountabilities

Executive Management Team
It is the role of the ICB Executive Management Team to define the ICB policy in respect of Information Governance, considering legislative and NHS requirements. The Executive Management Team is also responsible for ensuring that sufficient resources are provided to support the requirements of this policy.

BNSSG Information Governance Group (IGG)
The Information Governance Group (IGG) oversees and provides leadership within BNSSG ICB for Information Governance (IG), ensuring that it complies with statutory responsibilities and fulfils the requirements of data protection legislation. The IGG is responsible for the review of this Policy.

Chief Executive
The ICB Chief Executive has overall responsibility for Information Governance within the organisation. They are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. This includes assigning the role of SIRO and Caldicott Guardian roles. The Chief Executive is responsible for approval of this Policy.

Senior Information Risk Owner (SIRO)
The Senior Information Risk Owner for the ICB is a board member with allocated lead responsibility for the organisation’s information risks and provides the focus for management of information risk at executive management level. The SIRO will assign the role of DPO to a postholder. The Chief Executive must receive assurances from the SIRO that information risk is being managed suitably and successfully throughout the ICB, and for any services contracted by the organisation. The Caldicott Guardian, the Data Protection Officer, the IG Manager (SCW), and the Information Asset Owners (IAOs) provide support to the SIRO. The SCW Information Governance Manager will support the SIRO in fulfilling this role. In the absence of the SIRO there is a Deputy SIRO assigned by the SIRO.

Caldicott Guardian
The Caldicott Guardian is a member of the Executive Management Team and a senior health or social care professional with responsibility for promoting clinical governance or equivalent functions and advising on confidentiality issues. The Caldicott Guardian acting as the conscience of the organisation plays a key role in ensuring that the ICB satisfies the highest practical standards for handling patient/staff identifiable information. The Caldicott Guardian serves as part of a broader Caldicott function and is supported by the Data Protection Officer and SCW Information Governance Team.

ICB Digital Lead

The ICB Digital Lead is responsible for developing, managing, and implementing IT Security policies/processes daily and for managing arrangements relating to access/use involving the third-party IT supplier.

Data Protection Officer
When required the Data Protection Officer (DPO) will report directly to the ICB Board in matters relating to data protection assurance and compliance, without prior oversight by their line manager.

Directorate Information Governance Lead (DIG)
The Directorate Information Governance Lead role is a senior member of staff who has been identified by the responsible director to represent a ICB Directorate and support oversight of Information Governance processes. This includes providing support for the requirements of the Data Protection and Security Toolkit and awareness of this policy.

Information Asset Owners (IAO)
The SIRO and Directorate Information Governance Lead is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result, they can understand and address risks to the information assets they ‘own’ and to provide assurance to the SIRO that information risks within their areas of responsibilities are identified, recorded and that controls are in place to mitigate those risks. They will also investigate and act on any potential breaches of this policy.

Information Asset Administrators (IAA’s)
Information Asset Administrators are required to support the IAO’s and SIRO who will work with the SCW Information Governance Team to ensure staff apply the data protection legislation and Caldicott Principles and Information Governance and IT Policies within daily working practices.

SCW Information Governance Team
The SCW Information Governance Team supports the ICB and is responsible for ensuring that the Information Governance programme is implemented throughout the organisation. The team is also responsible for the completion and annual submission of the Data Security and Protection Toolkit. The Information Governance Team will support the organisation in investigating Serious IG Incidents Requiring Investigation (SIRIs), offer advice and support for the organisation to comply with this policy and support with communication through established channels including the intranet and staff briefings.

Local Organisational Administrator (LOA)
A Local Organisation Administrator (LOA) is responsible for managing local administrative tasks related to NHS.net connect accounts

ICB System Administrators
The System Administrator is responsible for the secure and efficient operation of the system. This includes managing user accounts and access permissions, ensuring compliance with NHS Information Governance standards. Additionally, they are accountable for facilitating audits.

Management
All managers are responsible for promoting good information governance within their team. This includes ensuring that staff complete induction training and annual Data Security and Awareness training and acceptance of this policy.

Line Managers will co-ordinate the leavers process to ensure the return of equipment and restriction of access to systems at the end of any employment or engagement with the ICB is initiated immediately.

All staff
All staff have responsibility for reading, downloading and complying with this policy and with Data Protection Legislation, organisational policies and for completing annual Data Security and Awareness training. Staff are also responsible for taking the necessary steps to maintain the security or equipment and data and for reporting breaches.

5 Definitions/explanations of terms used

AI System	Refers to foundational technologies that enable AI. They include the algorithms, models, and infrastructure that process data, learn from it, and make decisions. They form the backbone of AI capabilities, providing the tools and methods to develop intelligence behaviours
User	Any individual authorised to access and use IT and or AI systems provided or approved by the ICB, including employees, researchers, contractors, and other authorised personnel.
Organisational Data	Any information, data, or intellectual property belonging to BNSSG ICB
IT systems/apps	This includes all systems and applications deployed by the organisation for use, including the N365 platform.
Local Organisation Administrator (LOA's)	A Local Organisation Administrator (LOA) is responsible for managing local administrative tasks related to NHS.net connect accounts.
N365 Platform/Apps	The N365 platform refers to the Microsoft 365 suite of applications provided to the NHS, which includes tools like Word, Excel, PowerPoint, Outlook, OneNote, OneDrive, SharePoint, and Microsoft Teams. Microsoft 365 Products, Apps, and Services | Microsoft 365
Personal Data (Derived from the UK GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Special Categories of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to:

(Derived from the UK GDPR)	(a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to SCW or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

6 Principles

The user allocated and/or using the IT equipment, technology, systems/apps is responsible for its security and shall be liable for any inappropriate use.

- Users must not use any system/app for any purpose that conflicts with their contract of employment.
- Any user found violating this Policy shall be liable for the consequences of their actions and shall be subject to the ICBs disciplinary procedure.
- Any data residing on ICB equipment/systems is the property of the ICB, this includes corporate data stored on a personal device being the property of the employer, not the device owner.
- Users accept that personal use of ICB systems is not a right and must be exercised with discretion and moderation. Data must not be stored on personal devices.
- The ICB maintains the right to monitor the use of its systems/apps.
- The ICB can prohibit personal use of systems/apps without warning or consultation where evidence points to a risk to the ICB including a breach of this, or any other BNSSG ICB policy.
- The user allocated and/or using any systems/apps is responsible for its security and shall be liable for any inappropriate use.

- IT equipment, systems/apps must be used in compliance with all applicable laws, regulations, ethical guidelines, and the ICB's policies.
- IT systems must be used in a manner that respects the dignity, rights, and diversity of all individuals. You must not generate or disseminate content that is discriminatory, hateful, harassing, or otherwise harmful.
- Users are responsible for critically evaluating the output of AI systems and should not solely rely on AI-generated information without independent verification, especially critical tasks or decisions.
- Users must not input personal data, special category data, or confidential organisational data into any AI technology.

7 Conditions of Use

7.1 General IT use

All users of BNSSG ICB IT technology/systems/apps, as a condition of use, are required to:

- Be aware that usage monitoring and reporting is undertaken.
- Be responsible for maintaining the security of their accounts, and any data they access or process.
- Ensure multi-factor authentication is enabled, where possible.
- Only use ICB equipment/systems for limited personal use at the discretion of the user’s manager provided this never:
    - interferes with ICB work.
    - relates to a personal business interest.
    - is unlawful.
    - brings the ICB into disrepute or has potential to bring the ICB into disrepute.
- Not access any ICB information, data, or systems/apps they are not authorised to.
- Not attempt to circumvent or deliberately bypass any ICB security measures or controls.
- Accept full responsibility for the security of equipment and information which are issued to them, taking necessary precautions.
- Not leave devices unattended in a public place or left in sight in vehicles unattended or overnight.
- Be aware that USB memory sticks, flash memory cards and external hard drives, unless issued and approved by the ICB, are prohibited.
- Not install any hardware or software/apps on to the ICB laptop or desktop devices unless authorised and approved by IT service desk.
- Not change the configuration of any security settings on any ICB devices unless authorised by the IT service desk.

- Not remove or deface any asset registration number.
- Allow SCW IT Services to access devices to undertake any maintenance work.
- Seek appropriate permission before taking any ICB IT equipment outside the United Kingdom and take the necessary security measures if permission is granted.
- Must not store any personal identifiable data, special category or commercially confidential information on non-ICB supplied devices.
- Not store information permanently on portable devices. Where there is legitimate requirement to store data for secure transfer using portable media drive then use ONLY ICB-supplied encrypted memory sticks.
- Comply with the organisations password policy by not writing any passwords down and never sharing with other members of staff.
- Personal memory sticks must not be plugged into any corporate endpoints i.e., laptop, workstation, server, printer, or any network equipment unless authorised by IT service desk.
- Under no circumstances should PROTECT or RESTRICTED information be shared to your personal non NHS.net Connect (formerly NHS mail) email address or any other insecure address.
- Home/personal computers or laptops must not be connected to the organisation’s corporate network.
- Must ensure a call is logged, via the IT Service Desk, for the disposal of any equipment capable of storing sensitive data.
- Not accept, or run, software from non-trusted sources. If in doubt, please contact the IT Service Desk.
- Not undertake any activities with the intention of creating and/or distributing malicious programmes into corporate networks of systems.
- Not reject or disable automated security updates. Users must ensure all portable devices are connected to ICB networks either on site or through AOVPN to download security patches within 30 days of the last connection or their device may be disabled.
- Exercise diligence about cyber risks and take the necessary mitigating steps including through reporting suspicious activity and not opening unfamiliar links.
- Clinical data must be stored in clinical systems, however if documents need to be stored in Teams / SharePoint they must use sensitivity labels, be tagged appropriately, and have secure access permissions which are reviewed regularly.
- Ensure all documents that form corporate records are stored and managed in line with the organisational Records Management policy e.g., network drives/ folders or within SharePoint.

7.2 Unacceptable Use

The following activities are strictly prohibited:

- Excessive personal use in the working day is prohibited.
- Sharing personal, special data or ICB commercially confidential information with unauthorised individuals or external entities.
- Attempting to bypass (disable or change) any security measures, access unauthorised systems or data, or introduce malware (viruses, worms, spyware) into the ICB's environment.
- Do not access any ICB information or data you are not permitted to access.
- Inappropriate Content: Creating, storing, or sharing offensive, discriminatory, or inappropriate content, including but not limited to pornography, hate speech, or defamatory material.
- Misrepresentation: Misrepresenting oneself or others when using ICBs systems/apps.
- Commercial Use: Using systems/apps for commercial purposes without explicit authorisation from the Chief Digital Information Officer, or Deputy Digital Information Officer at the ICB once the Digital Team has been informed and approved.
- Violation of Intellectual Property Rights: Infringing on copyright, trademarks, or other intellectual property rights when using systems/apps, including submitting AI prompts that would lead to copyright infringement.
- Phishing and Social Engineering: Engaging in or facilitating phishing or social engineering attacks through systems/apps. Maintain caution and don’t open links that you are unfamiliar with.
- Unauthorised Software: Installing or attempting to install unauthorised software on ICB devices or within the N365 environment. If in doubt, before any attempt to install, check with IT Service Desk.
- The creation, use, transmission or encouragement of material, which is illegal, obscene, libellous (defamatory), offensive, threatening, harassing or discriminatory.
- Transmission of unsolicited commercial or advertising material or material which is detrimental to the work or reputation of the ICB.
- Any illegal activities including breaching General Data Protection Legislation, Computer Misuse and Design, Copyright and Patents Acts
- Violating or otherwise intruding upon other people’s privacy
- Willful disrupting other users’ work in any way, including with viruses or by corrupting data
- Any expression of personal views which could be misinterpreted as those of the ICB, or which are prejudicial to the interests of the organisation.

- Commit the organisation to purchasing or acquiring goods or services without proper authorisation.

The above list is not exhaustive and the use of BNSSG ICB supplied equipment for any inappropriate use is considered a serious breach of policy. Users should be aware that to do so could constitute a prosecutable offence under UK law. Improper conduct may lead to disciplinary procedures. If in doubt, please refer to the SCW Information Governance Team for advice before proceeding.

7.3 N365 Platform

This section sets out the ICBs approach and expectations for safe and secure use of the N365 platform throughout the organisation and provides guidelines on good etiquette for those using and accessing the platform and the data contained within it. The platform is described in the Glossary of terms.

- Only process data that is relevant for the purpose. Minimise the use of personal data, in particular Patient Confidential Data (PCD) and sensitive documents which are stored on N365 platform. Ideally Patient Confidential Data should be on a clinical system only, however where it is necessary to store within N365 there MUST be Role Based Access Control (RBAC) and other appropriate controls in place i.e. secure channels in Teams.
- No work-related data should be processed on N365 OneDrive. This must only be used to hold you own personal information.
- Be aware that “Allow everyone in your company” or “Organisation wide” settings will allow everyone in the NHS (with an email address suffixed with @nhs.net) on the National shared tenant to view the data. Setting permission to “Public” could provide direct access to the data from the internet and should not be used unless specifically approved by the Organisation’s Senior Information Risk Owner (SIRO) on Information Governance team or Deputy Data Protection Officer (DDPO) recommendation
- Regular review access permission you have created as part of the required audit process.
- MS Teams meetings created for one purpose MUST NOT be reused for another. For instance, senior management meetings and then reused for all staff meeting, leading to risk of inappropriate access to shared messages and documents.
- All data on N365 platform may be subject to Subject Access Requests (SAR) and potentially Freedom of Information (FOI) requests. This includes but is not limited to emails, MS Teams conversations, SharePoint data, OneDrive data.
- Staff must not install any Microsoft Office 365 software procured by the organisation on any unmanaged device unless approved by IT Service Desk.
- Staff MUST NOT use any other Internet based file sharing/storage applications unless explicitly approved by IT service desk, e.g., Dropbox, Google Drive.

7.4 Power Platform Development Standards and Best Practices

- Users must follow Power Platform best practices and development standards https://learn.microsoft.com/en-us/power-platform/well-architected/experience-optimization/design-standards to ensure the quality, maintainability, and scalability of their solutions.
- Solutions must be thoroughly tested before deployment to production environments.
- Documentation must be provided on all Power Platform solutions.

7.5 Power Platform Governance and Administration

- Users will be granted specific permissions and access levels based on their roles and responsibilities by the ICB Digital Lead.
- Changes to the Power Platform environment must be approved by the ICB Digital Lead.

7.6 Power Platform specific unacceptable use

- **Unauthorised Data Connections:** Connecting to data sources that have not been approved by the Information Governance team.
- **Circumventing Governance Policies:** Developing solutions that bypass or undermine the ICBs information governance policies, including data security, privacy, and access control.
- **Deployment without Approval:** Deploying Power Platform solutions to production environments without proper review and approval from the designated authorities.

7.7 Artificial Intelligence (AI)

BNSSG are committed to the responsible and ethical use of artificial Intelligence (AI) systems.

Please follow the AI Policy for use of AI and be aware of the following specific standards.

- AI software (e.g. Co-pilot) must not be used to process personal, special category or business confidential information.
- Understand the privacy policies and data handling practices of any third-party AI tools you are permitted to use.
- Ensure caution when sharing AI-generated content. Clearly indicate when content has been generated by AI if there is a risk of misinterpretation.
- Be responsible for the consequences of disseminating AI-generated content. If you share or publish content created by AI (like text, images, or data), you are accountable for how that content is used, interpreted, and the impact it may have.
- Do not present AI-generated work as your own unless explicitly permitted for specific educational or research purposes with proper attribution.
- Do not intentionally attempt to overload, disrupt, or damage AI systems.

- Report any suspected vulnerabilities or malfunctions of AI systems to the designated IT Service desk.
- Generating Unreliable Information: Relying on AI-generated content without verifying its accuracy and completeness. AI is a tool to assist, not replace, human judgment and fact-checking.
- Circumventing Governance Policies: Using AI in ways that bypasses or undermines the ICB's information governance policies, including data security, privacy, and access control.
- Submitting personal Data in Prompts: Directly inputting personal identifiable data into AI prompts is strictly prohibited. Anonymised or aggregated data may be used where appropriate and compliant with information governance policies.
- *Be mindful of the use of new and emerging technology and have a heightened awareness of potential risks despite perceived benefits.*
- *If in doubt, refer to IT service desk*

8 Equipment, data storage and access

- When leaving the workstation (desktop computer, mobile device terminal and laptops) for any period, the user must ensure they lock their computer session to prevent un-authorised access to the network and stored information *(Ctrl + Alt + Delete or 'Windows Key' + L).*
- All users must ensure their screens cannot be overlooked by members of the public, or individuals without the necessary authority when confidential data and/or information is displayed. Where appropriate, privacy filters should be used to protect the information or alternatively, relocate them to a more appropriate place.
- Care will need to be taken by staff working from home to ensure the security of both the information and hardware. This includes the security of a home office and equipment and the destruction of any sensitive printed material.
- All users are responsible for the information that is displayed on the screens whilst computer/laptop is being supported remotely by IT service desk or when in a webinar /Team's call.
- Following up to a maximum of 10 minutes of inactivity, the session will be automatically locked as a failsafe measure. This is set by SCW.
- Computers must be fully switched off and rebooted at least once per week to ensure vital updates are installed in a timely manner. Ideally this will be done daily, which will also support individual wellbeing and work life balance.
- Users are responsible for the safe keeping of equipment issued to them.
- ICB equipment must be returned on termination of employment or business relationship with the ICB or upon request.

- Users must not store files or folders on their C drive or portable drives.

9 Connecting remotely and mobile users.

- Users are provided with remote access; it is the user's responsibility to ensure that no unauthorised or inappropriate use (as defined in this policy) is made from those devices.
- Only remote access solutions that are provided or agreed with IT Services can be used to access ICB networks when away from ICB workplaces. Workstations which have remote access to ICB internal networks via the Internet must be protected from intrusion (for example, by locking screen or logging off when unattended, and ensuring passwords are not shared) to prevent unauthorised access to the ICB networks and systems. (SCW CSU IT support will provide advice and may supply approved solutions for use in such situations).
- Where initial set up arrangements are managed remotely and without connection to the ICB networks in one of its buildings, users are responsible for changing their login credentials immediately to ensure ongoing security.

10 Identities and Passwords

An individual identity profile will be allocated to users by SCW or the ICB (for specific systems and their administrators i.e. ISFE2 will be Finance) as part of set up procedures. This means that users are accountable for all actions performed under that identity.

Passwords and, if provided, security tokens or smartcards, are the keys to preventing others from misusing your identity:

- users will be allocated a unique user identity for the systems that they are permitted to use.
- users must not allow others to use systems under their identity and must keep passwords/smartcards /tokens secure.
- users are accountable for all actions performed under their identity.
- Users must use a password that conforms to 'strong' password rules. Passwords must contain capital and lower-case letters, numbers or non-alphanumeric characters.
- Users must not add additional passwords or security measures to any PC/laptop or files without first consulting with the IT service desk.
- Users must not attempt to modify, remove or bypass the password protection on any issued device.
- Users must not write down their username and/or password.

Where a user has reason to believe that their password has been disclosed to others, they must change it immediately and must report this as a potential security incident with the IT Service Desk who will determine if any immediate action is required.

See the **ICBs Password Policy** for detailed password policy statements.

11 Offensive and Inappropriate Material

The use of BNSSG ICB supplied equipment to access, store, copy or distribute items which are inappropriate, offensive, libellous (or in some other way illegal) or may jeopardise security in any way is prohibited. Users should be aware that to do so could constitute a prosecutable offence under UK law. Improper conduct may lead to disciplinary procedures.

12 Physical Security

Handheld and portable devices must be kept in your possession or locked away when not in use.

Laptops, mobile phones, and portable equipment must be transported securely (e.g., in the boot of a vehicle). Equipment must not be left in cars. Where for the purposes of transport or where leaving it in a vehicle is unavoidable equipment must be locked, out of sight either in the boot or a locked glove compartment.

Users must ensure that BNSSG ICB supplied equipment and workstations are installed in a physically secure premises building to protect them from theft and inappropriate or unauthorised use.

13 E-mail and Internet / Messaging Services

Like all correspondence, E-mail and instant messages cannot be regarded as purely private and only seen by the intended recipient. It may also be regarded as official correspondence of BNSSG ICB. Remember that E-mail can be stored, forwarded, and distributed to large numbers of people at the touch of a button, please consider whether all recipients ‘need to know’ before sending. Be aware that:

E-mail has been used successfully as evidence in libel cases and industrial tribunals. Sending defamatory mail, even internally, could make BNSSG ICB liable to pay heavy damages to injured parties.

It should also be noted that under the Right of Access under the UK GDPR (Article 15), an individual has the right to request disclosure of their personal details contained in E-mails and instant messages.

Before sending email, ensure that what is being sent is of an appropriate standard and is being distributed securely via NHS.net internal mail, or using the Egress secure messaging system’s [secure] subject line tag, to appropriate email addresses.

ICB users are encouraged to identify all personal emails by typing ‘personal/private’ in the email subject line, and file into a separate folder, against which regular housekeeping is performed, including the deletion of personal emails in a timely manner. The ICB’s Records Management provides guidance on the retention and destruction of work-related emails and records

To protect its interests and ensure compliance with regulatory or self-regulatory policies and guidelines, BNSSG ICB reserves the right to monitor the use of E-mail and the Internet and, where necessary, data will be accessed or intercepted. As part of routine IT practice certain websites are blocked. Restrictions will be made and can be lifted upon agreement to a request to the SIRO.

Certain use of the email and internet is prohibited and includes the following:

- use ICB's communications systems to set up or maintain personal businesses or to send personal or 'chain' letters, emails, or other messages.
- forwarding of sensitive ICB messaging to external parties without the documented appropriate permission.
- distributing, disseminating, or storing images, text or materials that might be considered indecent, pornographic, obscene, defamatory or that are illegal.
- distributing, disseminating, or storing images, text or materials that might be considered discriminatory, offensive, or abusive or might be considered as harassment or bullying.
- distributing, disseminating, or storing images, text or materials that may result in either reputational or commercial damage to the ICB, its subsidiaries, agents, or associated organisations.
- unauthorised access (electronic or physical) into any internal or external system.
- transmitting commercial or advertising material that is unsolicited by the recipient.
- undertaking deliberate activities that waste Employees' effort or system resources.
- deliberately or recklessly introducing or propagating any form of computer virus, spyware, or other malware.
- Intentional downloading of viruses or related security threats into systems.
- visiting internet sites or publishing content that may result in either reputational or commercial damage to BNSSG, its Employees, subsidiaries, agents, or associated organisations or would be deemed inappropriate by a senior colleague.
- using the computer to perpetrate any form of fraud related to software, film or video, music piracy or other copyright violation of any form.
- using the internet to store or publish material that could be considered discriminatory, offensive, or abusive or might be considered as harassment or bullying.
- publishing defamatory and/or knowingly false material about BNSSG, colleagues, NHS, or government Policy and/or the ICB's stakeholders.
- undertaking deliberate activities that waste Employees' effort or system resources.

The above list is not exhaustive and is considered a serious breach of policy which will be managed in line with HR Disciplinary Policy and/or criminal proceedings. Suspected attempts to access certain categories of site, specifically those which display any material likely to be illegal such as child abuse or obscene images which seek to deprave will result in immediate notification to the Police for investigation.

14 Use of Social Media and Social Networking

Social networking sites (such as Facebook, Twitter) are public forums the ICB wishes to embrace them as a demonstrable element of our commitment to a culture of openness. The communications team will provide guidance and training to empower staff to interact online in a way that is credible, consistent, transparent, relevant, and safe. Please refer to the ICB social media Policy for more information.

15 Incident Reporting

For the protection of ICB information and IT infrastructure and services, all employees and contractors have a duty to report all potential IT security incidents as soon as possible when they are discovered via the following:

- Their line manager, by phone, email or in person
- SCW CSU IT Service Desk
- Their departmental information asset owner, who will decide as to whether the incident should be reported onto Datix. If logged on to Datix, the CSU IG team will investigate the incident (please refer to ICB Information Incident Management Reporting Procedure).
- The following types of incidents must be reported:
- Any suspected misuse of BNSSG ICB computer systems, whether accidental or deliberate.
- A system or network security control that is (or is in danger of being) disabled or ineffective.
- A virus or malware infection is suspected on a workstation or server – note you must immediately turn the device off and then report it.
- Where a user discovers or suspects user behaviour which does not comply with the ICBs policies.
- Where a user suspects that personal and / or sensitive information is being disclosed or modified without proper authority.

Information received by line, section, or corporate managers regarding suspected or actual breaches of security will be treated confidentially.

16 Copyright and Licensing

Under the Copyright, Designs & Patents Act (1998) (the Act) the illegal copying of software is regarded as theft.

The rights of computer software designers/writers are protected by this Act. It is an offence to copy, publish, adapt, or use computer software without the specific authority of the copyright holders.

It is also important to be aware that all software or data files developed by staff on ICB computing equipment are the property of the ICB. They may not be made available for use outside of ICB without prior approval.

To comply with legislation, and to ensure ongoing vendor support, the terms and conditions of all licensing agreements must be adhered to. Where systems are provided through SCW this will be addressed as part of the contract. For additional software and system use further due diligence may be required and support can be obtained through SCW IT. All software and other applicable materials must be appropriately licensed whether installed or used on ICB or personal equipment.

Only Local Organisation Administrators (LOA's) are authorised to download new software and should seek advice from SCW IT before doing so.

As is the case in obtaining products by any other means, all licensing requirements, payment conditions and deletion dates associated with downloaded software must be met.

Anyone downloading software must be aware of the difference between:

- Copyrighted Software- requires a licence payment.
- Freeware - licensed but requires no payment.
- Shareware - copyrighted but often free for a trial period.
- Public Domain Software- which is free.

Any breach of the Act could result in disciplinary or even legal action. All software installed onto ICB devices must be obtained via official routes (e.g., from SCW IT) so that licences can be obtained and managed.

17 Third-Party Information

Some of the information a user receives or obtains from clients, suppliers and other third parties may be confidential or contain proprietary information. Like any other confidential information, the ICB has a duty to maintain its confidentiality and only use it for certain limited business purposes consistent with any applicable agreements which the ICB may have with the third party.

When making use of third party information users should be aware that such information may be protected by intellectual property rights (e.g. copyright under the Copyright, Designs & Patents Act 1988) and such usage may be subject to limitations and restrictions. Care is needed when sending attached files or reproducing information from the Internet.

Certain information may be subject to special provisions. Please refer to the ICB's policies on Freedom of Information and Individual Rights (which deals with Subject Access Requests. The ICB's website also carries the organisation's Privacy Notice identifying how data will be used.

18 Training requirements

All staff are required to undertake information governance training and download and read the ICBs information governance staff handbook and this Policy. All relevant material is contained on Consult OD. Additional relevant policies are available on the Hub, these include:

Line Managers are expected to deliver local induction to new starters including the familiarisation with IG/IT security requirements.

19 Equality Impact Assessment

Please see Appendix A.

20 Implementation and Monitoring Compliance and Effectiveness

Adherence to this policy will be monitored via investigation and analysis of information security incidents reported via the approved incident management process. This will include the number of incidents that relate to discrimination, harassment, or victimisation.

In addition, compliance with / awareness of this Policy will be monitored through the following mechanisms as part of the Data Security Protection Toolkit activities:

- Completion of the requirement to download and read the Policy on an annual basis.
- Annual IG training
- Completion of IG modules / training relevant to the roles of the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, Information

21 Countering Fraud, Bribery and Corruption

The ICB is committed to reducing and preventing fraud, bribery and corruption in the NHS and ensuring that funds stolen by these means are put back into patient care. During the development of this policy document, we have given consideration to how fraud, bribery or corruption may occur in this area. We have ensured that our processes will assist in preventing, detecting and deterring fraud, bribery and corruption and considered what our responses to allegation of incidents of any such acts would be.

In the event that fraud, bribery or corruption is reasonably suspected, and in accordance with the Local Counter Fraud, Bribery and Corruption Policy, the IG/IT Team will refer the matter to the ICB's Local Counter Fraud Specialist for investigation and reserve the right to prosecute where fraud, bribery or corruption is suspected to have taken place. In cases involving any type of loss (financial or other), the ICB will take action to recover those losses by working with law enforcement agencies and investigators in both criminal and/or civil courts.

22 References, acknowledgements and associated documents

- SCW CSU AUP Policy
- SCW CSU N365 Policy
- ICB Password Policy
- ICB Data Security and Awareness Staff Handbook
- SCW CSU Information Security Policy
- ICB AI Policy

23 Appendices

23.1 Appendix A - Equality Health Impact Assessment

EHIA for AUP Policy.pdf

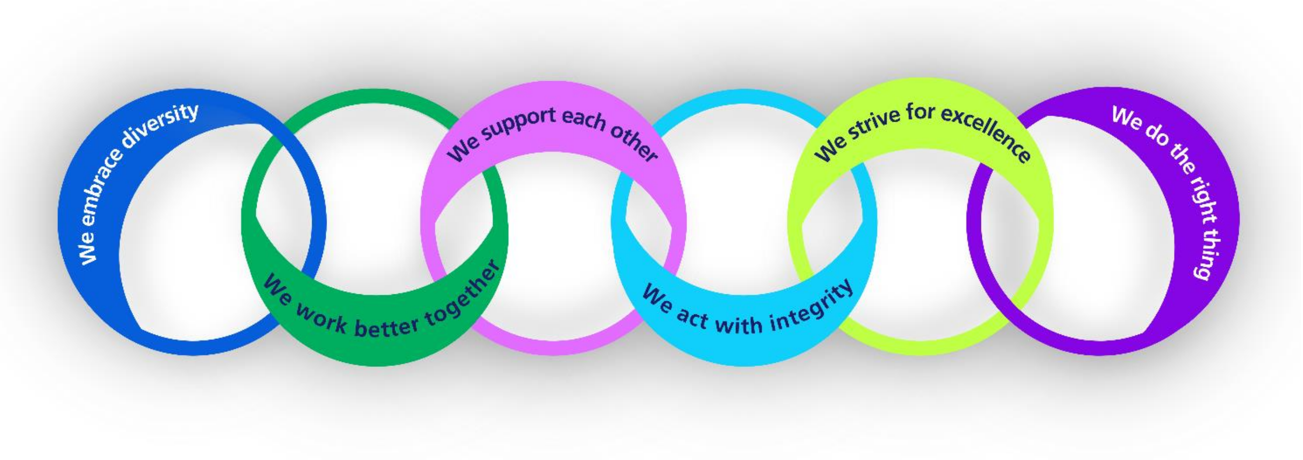
23.2 Appendix B - Implementation Plan

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
All staff	Launch of policy with briefing at HWGNFY	HWGNFY	[redacted]	Jan 26	Jan 26	Time on agenda
Directorate IG Lead	Aid dissemination and discussion with staff	DIGs meeting	[redacted]	Jan 26	Jan 26	None
All staff	Upload to Consult OD (Mandatory training requirement)	Send to Consult OD team	[redacted]	Jan 26	Jan 26	None
All staff	The Voice	Add information to the Voice	[redacted]	Jan 26	Jan 26	None
All staff	The Hub	Update version on the Hub	[redacted]	Jan 26	Jan 26	None

Healthier Together
Improving health and care in Bristol, North Somerset and South Gloucestershire

NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

Information Governance Staff Handbook



Together we are BNSSG

Author and Job Title:	SCW IG Team
Date Approved:	20th June 2025
Approved by:	[redacted], Senior Information Risk Owner Updates submitted to Directorate Leads and IAO/IAA Group and approval from IGG
Date of next review:	April 2027

Version Control

Version	Date	Consultation/Updates
1.0	12/02/2019	Corporate Policy Group, Staff Partnership Forum
1.1	September 2019	Update to NHS mail sections 6 & 7, Reference to removing fax machines, Updated DPO to [redacted], Updated working off site section (p18-19)
1.2	November 2019	Updated title, added "How can I access important emails or files from a colleague who is out of the office?"
1.3	February 2020	Update to Section 6, clarifying process for access emails accounts
1.4	September 2020	Updates to include arrangements for home working to support continued remote working due to Covid-19 and also email archiving.
1.5	November 2020	Updated to include Telephone Recording
1.6	July 2021	Added – section of working abroad and Website Blocking
1.7	August 2021	Updated section on Spam Email
2.0	August 2022	Updated contracts; removed reference to Fax safe havens; removed reference to mail safe. Updated ICB to ICB; updated to UK GDPR
2.1	January 2023	Update to contact details, links and standards. Addition of information on phishing emails.
2.2	March 2023	Additional advice recommended by ICO added the important of double checking attachments.
2.3	June 2023	Advice added in relation to autocomplete, working aboard, personal printers, Artificial Intelligence (AI). Approved by IAO/IAA meeting September 2023.
2.4	October 2023	Information Governance Staff Handbook Confirmation Slip removed. Change made to amount that can be fined.
2.5	February 2023	Change to email address (link broken)
2.6	January 2025	Renamed, update of roles, changes made to clarify key messages, amendment to working abroad and addition of section relating to new software/apps.
2.7	February 2025	Updated to consider IT/cyber, DPO and comments received from consultation, add reference to N365 Acceptable Use Policy

2.8	April 2025	Comments from IAO/IAA and Directorate Information Governance Leads added links to Hybrid Working Policy, addition of information about the use of names in public documents.

Contents

Information Governance Staff Handbook

Introduction

Information Governance (IG) is the practice by which organisations ensure information is efficiently managed and that appropriate policies, system processes and effective management accountability are in place to safeguard information.

Information Governance helps organisations to embed policies and processes to ensure that personal data and special categories of personal data, as defined in data protection legislation are:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Kept for no longer that is necessary and
- Processed in a secure manner.

Information Governance can also apply to corporate information and commercially sensitive data.

NHS organisations hold large amounts of personal, commercially confidential and special categories of personal data, and all staff should ensure that Information Governance standards are incorporated in their working practices. All organisations must be able to evidence their compliance with data protection legislation to fulfil the principle of accountability.

Personal and special categories of personal data can be contained within a variety of documents. For example:

- Health Records
- Staff Files
- Corporate Documents
- Commissioning Information

For the purposes of this handbook the use of the terms data and information are used to refer to distinct concepts and are not interchangeable.

Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'

Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'

Part 1 of this handbook provides a summary of the legislation and regulations that all staff should be aware of. Part 2 provide practical advice and information about key activities which will help to ensure compliance.

Part 1: Background & Legislation

1. Legislation and Regulations

Staff should know their responsibilities under the data protection legislation that governs how organisations use and safeguard data and information and how individuals can exercise their rights under that legislation. This area is complex but can be viewed as follows.

Data protection legislation is used as a generic term which encompasses the following:

- Data Protection Act 2018 (DPA 2018)
- UK General Data Protection Regulation (GDPR)
- Law Enforcement Directive (LED) (Directive (EU) 2016/680)
- Regulations made under the DPA 2018
- Any applicable national laws implementing them as amended from time to time
- All applicable law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

In addition, organisations must take account of the following legislation:

- Freedom of Information Act 2000
- Environmental Information Regulations
- Health and Social Care Act 2012
- Access to Health Records Act 1990
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988.

The organisation must also have regard for the following standards and Codes of Practice:

- International information security standard: ISO/IEC 27002: 2022
- Caldicott Principles
- Data Security and Protection Toolkit (dsptoolkit.nhs.uk)
- Cyber and data security - NHS Digital Data sharing information hub | ICO Codes of practice for handling information in health and care - NHS Digital
- Records Management Code of Practice
- Code of practice on confidential information
- Guide to Confidentiality in Health and Social Care
- Information security management NHS code of practice
- NHS Information Governance - Guidance on Legal and Professional Obligations - NHS England
- Confidentiality Supplementary Guidance - Public interest disclosures
- Anonymisation: managing data protection risk code of practice (ico.org.uk)
- Online safety | ICO.
- Data Sharing - Data sharing | ICO

The ICB also has a suite of Information Governance policies, processes and procedures, which can be found on The Hub.

Adherence to the principles of Information Governance supports compliance with the law and best practice. It also embeds processes that help staff manage data and information appropriately. It must also be noted that embedding Information Governance processes gives patients, service users and the public greater trust in the ICB and enables effective working across partner organisations.

2. Roles within the organisation

Chief Executive – [redacted]

The Chief Executive has overall responsibility for Information Governance legislation and best practices, and all the requirements within the 'Data Security and Protection Toolkit' within the organisation. They are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. This includes assigning the role of SIRO and Caldicott Guardian.

Senior Information Risk Owner (SIRO) – [redacted]

The Senior Information Risk Owner for the ICB is a board member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at executive management level. The Chief Executive must receive assurances from the SIRO that information risk is being managed suitably and successfully throughout the ICB, and for any services contracted by the organisation.

The Caldicott Guardian, the Data Protection Officer, the IG Manager (SCW), Directorate Information Governance Lead and the Information Asset Owners (IAOs) provide support to the SIRO. In the absence of the SIRO there is a Deputy DIRO assigned by the SIRO. The SCW Information Governance Team support the SIRO in fulfilling this role.

Caldicott Guardian - [redacted]

The Caldicott Guardian is a member of the Executive Management Team and a senior health or social care professional with responsibility for promoting clinical governance or equivalent functions and advising on confidentiality issues. The Caldicott Guardian acting as the conscience of the organisation plays a key role in ensuring that the ICB satisfies the highest practical standards for handling patient/staff identifiable information. The Caldicott Guardian serves as part of a broader Caldicott function and is supported by the Data Protection Officer and SCW Information Governance Team. SCW Information Governance Team support the Caldicott Guardian in fulfilling this role.

Data Protection Officer – [redacted] (Acting)

When required, the Data Protection Officer (DPO) will report directly to the ICB Board in matters relating to data protection assurance and compliance, without prior oversight by their line manager. The DPO will routinely report to the Information Governance Group with matters flowing to the Audit and Risk Committee as required

The DPO must ensure that their responsibilities are not influenced in anyway and should a potential conflict of interest arise report this to the highest management level.

The Data Protection Officer (DPO) is the person within the ICB that will ensure that Information Governance incidents which are likely to result in a risk to the rights and freedoms of individuals the ICO (Information Commissioner's Office) is informed within 72 hours.

SCW Information Governance Team

SCW provides IG support services in line with the information governance service specification under any Service Level Agreement for IG Service.

Directorate Information Governance (IG) Leads

The Directorate Information Governance Lead role is a senior member of staff who has been identified by the responsible director to represent a ICB Directorate and has responsibility for Directorate compliance to Information Governance processes. This includes being a member of the ICB Information Governance Group and providing support for the requirements of the Data Protection and Security Toolkit and awareness of Information Governance policies.

Information Asset Owners (IAO)

The SIRO and Directorate IG leads are supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result, they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The SCW Information Governance Team will support the IAOs in fulfilling their role.

Information Asset Administrators (IAA's)

Information Asset Administrators are required to support the IAO's, Directorate IG lead and SIRO who will work with the SCW Information Governance Team to ensure staff apply the data protection legislation and Caldicott Principles within daily working practices.

3. Definitions of terms used

Commercially Confidential Data/Information	Business/Commercial data or information, including that subject to statutory or regulatory obligations, which may be damaging to the ICB or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the GDPR (meaning as defined in chapter 2 (6) of the Data Protection Act 2018).
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the GDPR.
Special Categories of Personal Data	of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject

	(b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether individuals are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life.

4. Caldicott and Data Protection Legislation Principles

The National Data Guardian made recommendations to improve the way the NHS uses and protects confidential information in the form of the Caldicott Principles. All NHS employees must be aware of the principles which apply to both patient and staff data.

Principle 1: Justify the purpose - Why is the information needed?

Principle 2: Don't use personal confidential data unless absolutely necessary – Can the task be carried out without identifiable information?

Principle 3: Use the minimum necessary personal confidential data – Can the task be carried out with less information?

Principle 4: Access to personal confidential data should be restricted to required/relevant personnel.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities – Lack of knowledge is not acceptable

Principle 6: Understand and comply with the law.

Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality

Principle 8: Inform patients and service users about how their confidential information is used

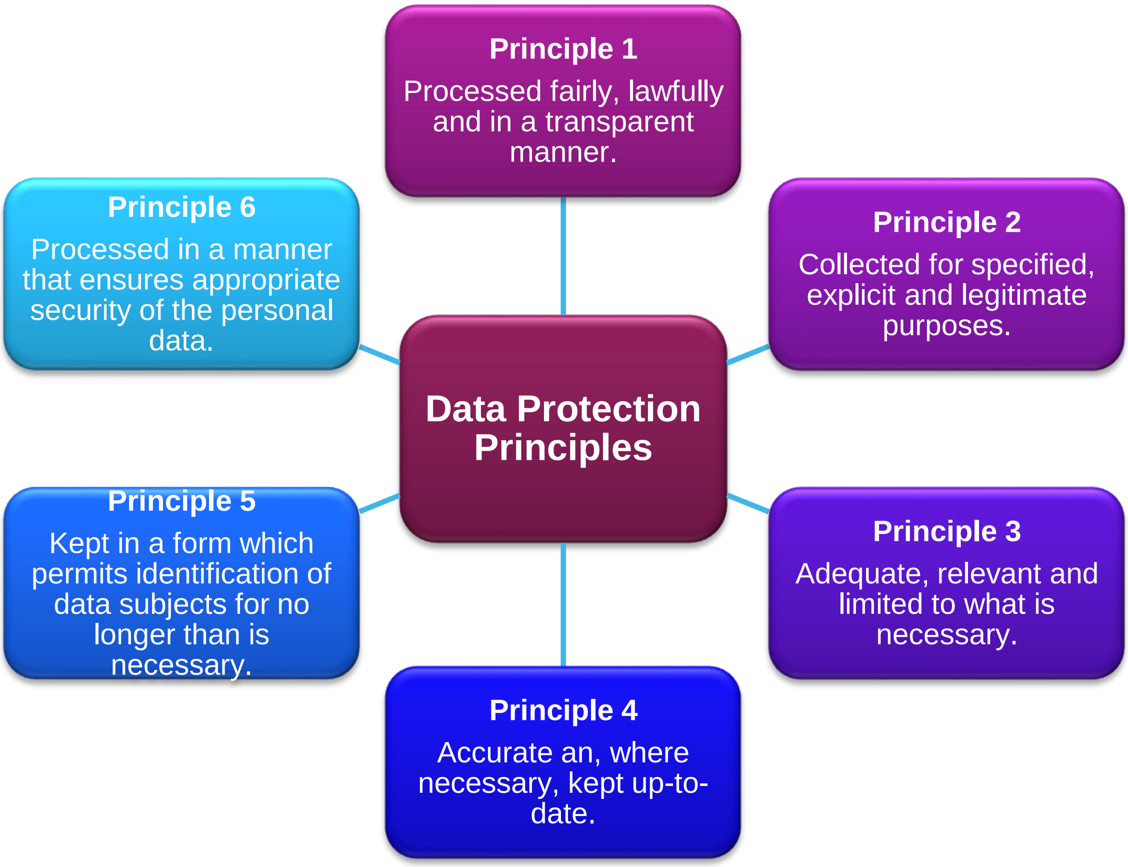
Data Protection Legislation and Principles

All organisations in the UK must comply with the data protection legislation which is defined in the Data Protection Act 2018 part 1(3)(9). The data protection legislation is enforced in the UK by the Information Commissioner's Office (ICO) who has the power to impose penalty notices on organisations.

Under the legislation it is not just data breaches which can attract a fine, non-compliance with the regulations can also be subject to fines which is why under the recording additional new data protection concept of ‘accountability’ organisations must be able to provide evidence of compliance.

Accountability: GDPR Article 5 (2) “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

The following are the six Data Protection Regulation principles (Article 5) that must be followed when handling personal and special categories of personal data. These principles should be considered when handling both corporate and clinical records.



Data Protection Principles

Principle 1
Processed fairly, lawfully and in a transparent manner.

Principle 2
Collected for specified, explicit and legitimate purposes.

Principle 3
Adequate, relevant and limited to what is necessary.

Principle 4
Accurate an, where necessary, kept up-to-date.

Principle 5
Kept in a form which permits identification of data subjects for no longer than is necessary.

Principle 6
Processed in a manner that ensures appropriate security of the personal data.

In addition, the Data Protection Legislation requires the ‘controller’ (see definitions above) to demonstrate compliance with these principles.

Data protection legislation and the Caldicott principles translate into **key rules for all staff to follow:**

- Patients and staff must be fully informed about how their information may be used.
- There are strict conditions under which personal and special categories of personal data may be disclosed.

- Individuals have rights including the right to information, the right of access, the right to rectification and erasure, the right to restrict processing, the right to data portability and the right to object to various types of processing of their data.
- Identifiable information should be anonymised or pseudonymised wherever possible.
- The disclosure or sharing of personal data is permissible where there is a legal obligation to do so, or an exemption can be applied or where the individual has given explicit consent.
- Sharing of personal data between organisations can only take place with appropriate authority, safeguards and agreements in place.
- Sometimes a judgement must be made about the balance between the duty of confidence and disclosure in the public interest. Any such disclosure must be justified.
- Personal data should be always kept secure and confidential.
- An organisation must be able to provide evidence to show compliance with the data protection legislation.

5. Confidentiality

Everyone working in or for the NHS has a responsibility to use personal data and information in a secure and confidential way. Staff who have access to data and information about individuals (whether patients, staff or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality. This guide sets out the key principles and main ‘do’s and don’ts’ that everyone should follow to achieve this for all types of records.

The common law of duty of confidentiality requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to, unless there is a statutory or court order requirement to do otherwise.

What is Personal Data?

Part 1, subsection 3 of the Data Protection Act 2018 provide definitions:

(2) “Personal data” means any information relating to an identified or identifiable living individual.
(3) “Identifiable living individual” means a living individual who can be identified, directly or indirectly, in particular by reference to—

> (a) an identifier such as a name, an identification number, location data or an online identifier, or
>
> (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

What are Special Categories of Personal Data?

Article 9 of the UK GDPR states that special categories of personal data are personal data revealing:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) the processing of genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health or
h) data concerning a natural person’s sex life or sexual orientation.

Under data protection legislation staff can only process or access personal data if:

- An appropriate condition for processing (under UK GDPR Article 6 and Article 9) and a supporting lawful basis has been identified and documented (Data Protection Impact Assessment - DPIA) or,
- Explicit consent has been obtained from the individual or,
- The data has been anonymised or pseudonymised or,
- The data is in respect of safety, safeguarding or in the public interest.

Any decision taken to share or publish personal or special categories of personal data that is by its nature, owed a duty of confidentiality should be discussed with the SCW Information Governance Team or DPO and documented in a DPIA (where necessary).

Staff should check with the SCW Information Governance Team if they have any queries on whether to share, access or process personal or special categories of personal data.

Personal Confidential Data

Although an organisation within the NHS may have identified a lawful basis to process data, including special categories of personal data, this does not necessarily mean that the data or information can be used or shared in a way that identifies the individual if that information has been obtained where a 'duty of confidence' is owed.

In practical terms this means that if a GP wanted to share information with another care organisation that is providing care to that patient e.g. an acute or community hospital, as long as the GP believes that the patient would raise no objection and that it would be within their reasonable expectations for them to do this then this sharing is permitted and encouraged within the law. If, however, the GP wishes to share information that identifies a patient and was obtained confidentially with someone else e.g. a charity, an advocate or the ICB, unless there are reasons why this must happen due to statutory obligations or it is in the public interest to do so, the patient must be given the opportunity to consent to this happening.

It may be easier to consider the following:

What information?	Category of data	How was it obtained?	Is it confidential?
Name, address and postcode	Personal Data	Electoral register	No
Full Postcode, recent hospital admissions, age, marital status	Personal Data and Special category of personal data	Performance report	Yes – measures to reduce the risk of identifying the person should be taken by reducing the postcode search criteria
Member of local church	Special category of personal data	Facebook members group post	No – made public by the individual
Religious belief limiting health care	Special category of personal data	Patient to GP consultation	Yes – GP would only share if patient would expect this for their care

Date of surgery on knee	Special category of personal data	Individual posted photo of themselves in hospital	No – made public by the individual
Date of surgery on knee	Special category of personal data	GP included in request for further funding for additional operation	Yes – GP would only share if patient would expect this for their care
Sexual orientation	Special category of personal data	Identifies own orientation on social media or other public forum	No – made public by the individual
Sexual orientation	Special category of personal data	Consultant includes information on gender reassignment status within hospital record	Yes – highly confidential and consultant would only share if patient would expect this for their care or has given explicit consent

Commercially confidential data

This describes information that is owed a duty of confidentiality concerning the organisation and its business. This includes trade secrets, parts of the procurement and contracting process and also information it may hold that has been given to it by a third party.

Part 2: Practical Advice

1. What is an Information Sharing or a Data Sharing Agreements and do I need one?

It is important to ensure that there is a balance between sharing information with others and keeping information secure and confidential. The ICB needs to ensure that mechanisms are in place to enable reliable and secure exchange of data within the legal limits.

A Data Sharing Agreement (DSA) should be put in place where several controllers wish to share information or data for a common purpose. An example of this could be a group of ICB's who want to share information across all their geographical areas to look into the use of an acute hospital. The agreement must include the lawful basis for sharing the information and be clear on the responsibilities of each organisation in relation to that information. Advice can be sought from the SCW Information Governance Team and agreements must be approved the Caldicott Guardian.

Data Sharing Agreements document must include:

- The purpose for the information to be shared/purpose of the agreement
- What information will be shared
- Who the information will be shared with
- Senior Management/Executive endorsement of data sharing agreement
- Structures of sharing information
- The legal basis in which the information is being shared in adherence to the Data Protection Legislation.

For further advice and guidance on DSA's, please contact the SCW Information Governance Team who will be able to provide a standardised template for you to adapt to the situation where information is being shared.

2. What is a Data Processing Agreement?

Whenever a Controller uses a Processor (a third party who processes personal data on behalf of the Controller) it needs to have a written agreement in place, this is known as a Data Processing Agreement. Similarly, if a Processor employs another Processor it needs to have a written agreement in place.

Agreements between Controllers and Processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the legislation. The use of agreements by Controllers and Processors may also increase data subjects' confidence in the handling of their personal data and information.

Agreements must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Agreements must also include a number of standard terms which have been included in a standardised template DPA that is available from the SCW Information Governance Team. It is important to remember that every processing activity may be different and whilst there will be common agreements in place e.g. between BNSSG and SCW, each might need to be assessed through the completion of a DPIA to ensure that no changes are needed to the standard template.

If a Processor fails to meet any of the obligations in the agreement or acts outside of against the instructions of the Controller, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

If a Processor uses a sub-processor, then it will, as the original Processor, remain directly liable to the Controller for the performance of the sub-processor's obligations.

Any signed agreements must be sent to the SCW Information Governance Team to ensure the ICB has a register of agreements.

3. What is a Data Protection Impact Assessment (DPIA) and do I need to complete one?

It is important to consider IG implications when starting new projects and programmes that involve the use of data/information. You should involve the SCW Information Governance Team at programme and project initiation stage to identify the IG elements that should be considered. This may include a Data Protection Impact Assessment (DPIA) which under the data protection legislation is a statutory requirement where processing of personal information is likely to result in a high risk to the rights and freedoms of individuals and in the cases of:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing
- Processing on a large scale of special categories of data or
- Systematic monitoring of a publicly accessible area on a large scale.
- Use of artificial intelligence (AI) software to process personal data

A DPIA assesses a project or piece of work and identifies Information Governance risks or requirements. A template, guidance documents and other checklists to help with a DPIA are available from the SCW Information Governance Team. The template includes a list of screening questions which are to be used to identify whether a full DPIA is required. In line with Data Protection Legislation the SIRO and/or DPO must be included and advise on the proposed processing as part of the DPIA completion.

Identifying Information Governance elements at an early stage will help to ensure:

- Compliant operations
- Necessary information sharing protocols and data processing agreements are in place
- BNSSG is aware of and can effectively monitor the use of information and data.

It will also limit the potential of failing to comply with the Data Protection Legislation and subsequent notices from the Information Commissioner's Office (ICO). The ICO can impose a penalty for failing to complete a DPIA.

Once the DPIA has been completed, the document must be forwarded to the SCW Information Governance Team for review/comment/recommendation. All DPIA are approved by a Senior Information Governance Consultant and the Deputy Senior Information Risk Owner or equivalent.

4. What rights do individuals have under the data protection legislation?

The UK GDPR confers rights on individuals that can be exercised in certain circumstances, these rights are:

a) **The right to be informed (articles 12 to 14)**
This means that the Controller should provide information to individuals about how their personal information is processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language, considering the age of the audience (e.g. children). This is usually done through a Fair Processing Notification (FPN) which will be on an organisation's webpages, on posters or leaflets or using a mixture of all of these methods. There are certain criteria that need to be met, and specific information included. Ask the IG team for more information or go to ICO guidance - right to be informed

b) **The right of access - Subject Access Requests (article 15)**
Under the data protection legislation individuals have a right to be informed of the following:

- Whether the ICB holds, stores or processes personal data about them
- A description of the categories of data held, the purposes for which it is processed and to whom it may be disclosed
- A copy of any information held
- What the source of the data held is
- Where automated decision-making has taken place, data subjects must be informed about the logic involved and envisaged consequences of such processing for the Data Subject.

Copies of records requested must be made available free of charge unless the request is manifestly unfounded or excessive, particularly if it is repetitive.

Requests must be sent to the Information Rights team who will process the request: bnssg.foi@nhs.net

As a staff member, you can obtain your personal information through the HR team, you must follow this process. If you access your own personal information directly through systems used within BNSSG disciplinary action will be taken.

c) **The right to rectification (article 16 and 19)**
An individual can exercise the right to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. You have one calendar month to respond to a request. In certain circumstances you can refuse a request for rectification.

d) **The right to erasure (article 17 and 19)**
An individual has the right to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. You have one month to respond to a request. The right is not absolute and only applies in certain circumstances.

e) **The right to restrict processing (article 18 and 19)**
Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, you are permitted to store the personal data, but not use it. An individual can make a request for

restriction verbally or in writing. This right has close links to the right to rectification and the right to object.

f) **The right to data portability (article 20)**
The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the midata[1] system and similar initiatives which allow individuals to view, access and use their data.

g) **The right to object (article 21)**
Individuals can object to processing of their information based on UK GDPR conditions of legitimate interests, performance of a task in the public interest, direct marketing, and processing for purposes of scientific/historical research and statistics.

If requested you must stop processing the personal data unless: you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is in relation to legal claims. You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

h) **The right not to be subject to automated decision making and profiling (article 22)**
The UK GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

You can only carry out solely automated decision-making that has legal or similarly significant effects on them this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by European Union or Member state law applicable to the Controller; or
- based on the individual's explicit consent.

You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:

✓ give individuals information about the processing
✓ introduce simple ways for them to request human intervention or challenge a decision
✓ carry out regular checks to make sure that your systems are working as intended.

5. What can I do to help keep information secure and confidential?

I. **Know BNSSG's organisational arrangements including key IG job roles:**
SIRO: [redacted]
Deputy SIRO: [redacted]
Data Protection Officer: [redacted]
Deputy DPO: [redacted]
Caldicott Guardian: [redacted]
Your Directorate **IG Lead**

[1] https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment

Your team **Information Asset Owner**
Your team **Information Asset Administrator**
IG Service Lead: [redacted]

II. Limit unnecessary access to personal information

- Do not discuss confidential matters outside of work, or with anyone at work who does not need to know; be aware that other people may overhear.
- Do not leave working papers lying around at home or in the office
- Hold swipe cards, keys and other access means, such as combination of locks, securely away from the point of storage when not in use. Ensure that there is an appropriately secure system in place to allow access in event of emergency or an individual's absence.
- Keep workstations and other computer equipment secure, being particularly careful with laptops when not in use
- Where possible lock away portable devices.
- Do not write down your passwords or share them with anyone.
- When viewing confidential information, you should ensure that your screen cannot be seen by unauthorised people
- Do not leave your PC unattended whilst it is logged-in when working in any location. Lock your screen every time you leave your desk (Ctrl+Alt+Delete or 'Windows Key'+L).

III. Ensure authorised access only

- Access to records must be on a "need to know" basis only.

IV. Follow accuracy, retention and disposal requirements

- If adding information to records, ensure accuracy and relevance; any queries should be raised with the Directorate Lead or Information Asset Owner.
- If you are an Information Asset Owner, ensure that records are held in accordance with the ICBs Records Management Policy The appropriate retention schedule must be documented on the Data Flow Map and Information Asset Register for the area.
- Ensure any personal or special categories of personal data are confidentially disposed of. Ordinary waste bins and recycling bins should not be used for any documents containing personal, commercially confidential or special categories of personal data.
- Dispose of redundant equipment, especially disk or tape copies of personal, commercially confidential or special categories of personal data, in the proper manner through the ICBs IT Delivery Partner (SCW CSU).

V. Take precautions when working off-site (this includes when working from home)

- Do not take personal, commercially confidential or special categories of personal data out of the office unless authorised.
- If you are authorised to take information off-site, always make sure that a list of the records/information that you take off site is retained at your base and your line manager is aware.
- Always protect the security and confidentiality of the information. If records are taken off-site by agreement, they should be transported out of sight in the boot of the car and removed to a place of safety on arrival at your destination.
- Be mindful of where you are working and what information might be visible to others in the environment. Take steps to adequately prevent inadvertent access to the information.
- Avoid printing any personal, sensitive or confidential business information on your personal printer. If this activity is undertaken, please ensure any data is kept confidential.

VI. **Action any requests for information**

If you receive a request for information about the organisation refer to the FOI section below. For requests relating to a patient, staff member, etc. and where it is not usually part of your job to respond refer to the Individual Rights Request section.

VII. **Do not misuse data to which you have access**

- Do not pass any information to your own relatives or friends, and do not attempt to find out details about them.
- Do not pass on any information for personal or commercial gain.
- Do not attempt to access your own records on any system unless through the appropriate procedure (via HR).

VIII. **Only disclosure information to third parties when authorised to do so**

You may, as part of your job, need to disclose patient/personal information to others:

- Keep the amount of information disclosed (even within the NHS) to the minimum necessary.
- Do not duplicate records, (on paper, or in a computer) unless essential for the purpose.
- Ensure that information that contains personal, confidential and special categories of personal data are only disclosed in accordance with the law, after a DPIA and any relevant and necessary agreements are in place; if in doubt, refer to the SCW Information Governance Team.
- Check the consent of document before they are published and ensure personal data is removed where necessary.

IX. **Take care when processing patient details**

- Do not leave messages that contain personal, commercially confidential or special categories of personal data on home answering machines as it may not be the person for whom the message is intended for.
- White boards or other displays that contain personal, commercially confidential or special categories of personal data should not be visible to the public or those without need to know.
- Any notes containing personal, commercially confidential or special categories of personal data written whilst taking a phone call or other message should be destroyed securely.

X. **Transfer information securely**

The ICO has imposed monetary penalties, warnings, reprimands and enforcement notices on organisations who have failed to comply with the Data Protection Legislation due to insecure transfers of information via instant messages, post and emails. In order to prevent this occurring within the ICB, it is the responsibility of each individual member of staff to ensure that the necessary processes are followed when transferring information.

6. What should I do to archive my emails and stop my email account from becoming full and blocked?

Our email accounts contain vast volumes of information that is vital for our daily activities; we need to ensure that this information is managed appropriately and in line with our policies. We need to make sure that information is available when needed whilst at the same time ensuring that information is not being kept longer than required. Please follow advice below:

1. Set aside time to review your emails.

2. Refer to our Records Management Policy on the Hub and use the embedded retention schedule to help decide whether information can be destroyed or needs to be retained.
3. Do not use your email systems as a record management tool.
4. Save a copy of any key emails and/or attachments in an appropriate folder on the network drive/system, files and emails can be ‘dragged and dropped’ to the suitable network location. Please ensure that files on the network are named appropriately so that they are easily located. This ensures that important information is accessible by colleagues and that you do not fill your email account with large attachments. Once a copy has been saved in the shared network location, these emails can be deleted from Outlook
5. Identify duplicates; drafts and superseded messages that can be deleted
6. Delete emails when they are no longer required for operational purposes and are not the primary or only version of a record that we are required to retain in line with the retention schedule.
7. Remember to regularly empty your deleted items folder
8. Don’t forget to delete sent items as well when they are no longer needed, especially if they include large attachments.
9. Once the above steps have been taken and you have identified remaining emails within outlook that need to be retained then you can use Exchange Online Archiving to archive emails and save space in your email account.

7. How can I access important emails or files from a colleague who is out of the office?

On occasion there may be a need to access an individual’s email account or folders. Such occasions will be in exceptional circumstances and must always be for an identified purpose. Such circumstances could include a prolonged period of absence where the absence is affecting ICB operation or when an individual has left at short notice.

Authority to grant access to an individual’s information must be approved by the SIRO (or Deputy) and/or Caldicott Guardian who will consider whether there is a strong, legitimate and specific business need to access the account.

Evidence of this approval should be shared with the IT helpdesk who can provide access. Access will be provided by delegate access, and no passwords will be shared. Access will be time limited and good practice is to have two people access the files together to prevent misuse. Only information that falls within the identified purpose should be accessed.

When an individual who has a BNSSG sponsored nhs.net email account leaves, the account can be transferred or disabled. Disabled accounts cannot be transferred between organisations. If an account is disabled and access to it by another member of staff is required, this can be arranged.

Authority to grant access to a disabled email account must be approved by the SIRO (Deputy) and/or Caldicott Guardian who will consider whether there is a strong, legitimate and specific business need to access the account. Evidence of this approval should be shared with the IT helpdesk who can provide access. It is not possible to grant access to an account that has transferred with an individual to another organisation.

8. Can I move my NHS mail account between organisations?

All staff are responsible for managing their emails and calendars in accordance with Information Governance principles and the NHSMail Acceptable Use Policy. The policy states:

"When moving your NHSmail account between health and care organisations, it is your responsibility to ensure any data relating to your role is archived appropriately and is not transferred to your new employing organisation in error."

Therefore:

- if you are new to the organisation and have brought an NHS mail email account with you from previous employment you must ensure that it is cleared of all confidential information relating to your previous role and employment. You will also need to review any delegated access to any calendars, inboxes, shared calendars or teams' sites to ensure that that only ICB colleagues have access to them.
- if you are leaving the ICB and wish to take your email account with you, you must ensure that you delete all information relating to your role within the ICB unless you have gained permission to take the information with you from your line manager. You will also need to review any delegated access to calendars or inboxes and shared calendars to remove any ICB colleagues.
- remember that if you embed any documents into meetings in your calendar, that these documents will be viewable and can be opened by anyone who has access to your calendar, so you should ensure that documents that are sensitive or confidential are not included. Consider also what you name your meetings and take account of any sensitive information eg in relation to meetings regarding staffing issues.

It is ICB policy that ICB allocated email addresses must be used for ICB Business, where staff work for multiple organisations separate emails address should be used to ensure that all ICB records are separated and can be managed according to ICB policy.

9. How do I use NHSmail to send information securely?

It is policy that emails containing any confidential or commercially sensitive information should be sent using an NHS.net account. If you're emailing from your @nhs.net account to another @nhs.net account, then you can be confident that the content of your message is encrypted and secure.

The table below is a summary of email addresses that are known/not known to be secure. Emails to secure addresses are encrypted in transit and the receiving organisation has committed to protect the data upon receipt. The secure e-mail standard is updated monthly and if you are in any doubt as to the security of the mail address you are using then you are advised to check here on a regular basis for Sharing Sensitive Information.

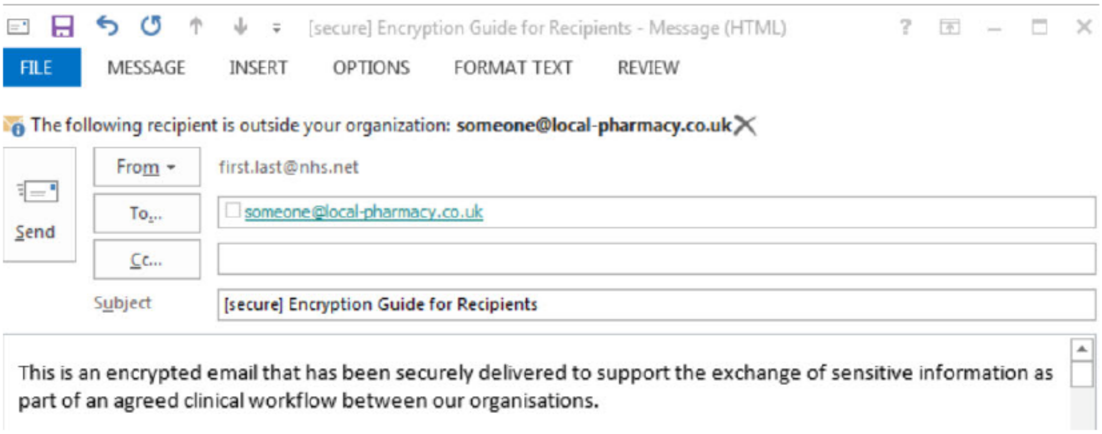
Recipient email address ends	Secure	Additional actions required
nhs.net	Yes	Secure – no additional action required
secure.nhs.uk	Yes	Secure – no additional action required
nhs.uk (does not end secure.nhs.uk)	Unknown	Use [secure] in the subject line
gov.uk	Yes	Secure – no additional action required
Cjsm.net	Yes	Secure – no additional action required
pnn.police.uk	Yes	Secure – no additional action required
mod.uk	Yes	Secure – no additional action required
parliament.uk	Yes	Secure – no additional action required

Any other email address	Unknown	Use [secure] in the subject line

Guidance for sending emails to non-secure domains.

When sending emails with confidential data outside of NHSmail you must use [secure] in the subject line of your email (the word secure must be in square brackets as in screenshot below), [secure] is not case sensitive. The Encryption Guide for NHSmail must be followed to ensure you understand all guidance and instructions on using this feature.

Example screen shot below:



The following recipient is outside your organization: someone@local-pharmacy.co.uk

From: first.last@nhs.net

To: someone@local-pharmacy.co.uk

Subject: [secure] Encryption Guide for Recipients

This is an encrypted email that has been securely delivered to support the exchange of sensitive information as part of an agreed clinical workflow between our organisations.

Guidance for Accessing Encrypted Emails

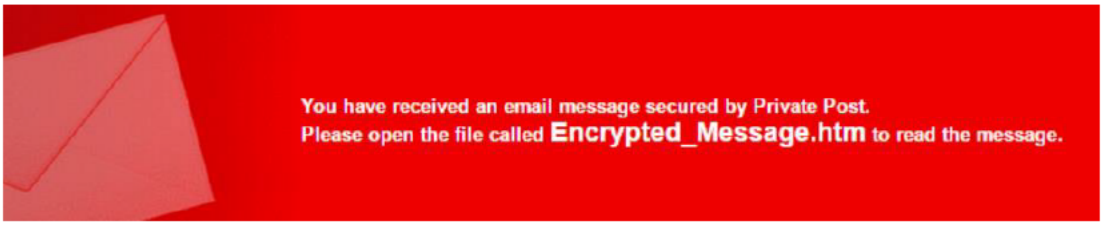
An encrypted email sent from an NHSmail address (ending @nhs.net) will contain a link to access the encrypted message.

PRIVATE AND CONFIDENTIAL

You have received an email

message secured by Private Post. Please open the file called

(*example of an* encrypted NHSmail email message)



You have received an email message secured by Private Post.
Please open the file called **Encrypted_Message.htm** to read the message.

(*example of an* encrypted NHSmail in Gmail)

The NHSmail Accessing Encrypted Emails Guide must be followed to ensure the recipient follows the registration process to set up with an account with the NHSmail encryption provider. The Guide also provides advice on replying and forwarding encrypted emails.

The NHSmail portal (https://portal.nhs.net), NHSmail Support Site will provide you with information and guidance on sending and receiving emails outside the NHSmail service – please refer to the Sharing Sensitive Information Guidance.

As a user of the NHSmail platform you must operate in accordance to the published guidance, policies and procedures to ensure you are using NHSmail effectively, appropriately and safely. Please refer to the materials below to ensure you are adhering to NHSmail guidance:

- NHSmail Acceptable Use Policy (AUP)
- Information Management Polices
- Sharing Sensitive Information Guidance
    - Encryption Guide for NHSmail
    - Accessing Encrypted Emails Guide
    - Encryption Guide for Senders.

Do not put personal confidential or special categories of personal data in the subject header when sending an email.

Please seek advice from the SCW Information Governance Team if required.

E-mail guidance:

- It is important to double check attachments and hyperlinks when communicating both internally and externally.
- Double check email recipients before sending the email. Remember Outlook may try and predict the recipient of the email based on the first few letters of the email address. There is an option to turn off auto complete when sending email in Outlook if this is your preferred option,
- Check what you are 'forwarding' or sending, when using the 'reply all' option in case the information is not intended for further sharing.
- Ensure that any attachments do not include information that should not be shared such as hidden tabs of individuals names or identifiers.
- Make sure you select the correct recipient from the address book.
- Remember that any email you send that contains information about an identifiable individual could be disclosed under the right of Subject Access (see below).
- Sending ICB information to private or personal email accounts should be avoided
- Don't overuse the 'cc' option, only send to those who need the information and not 'just in case'.
- Think very carefully about using the 'Bcc' option, it is appropriate for protecting the anonymity of recipients but not in every situation.
- Multi Factor Authentication (MFA) must be used when using NHSMail: https://support.nhs.net/knowledge-base/self-enrol-for-multi-factor-authentication-mfa/. MFA will help protect your account from compromise, even if your password was discovered, and will notify you if unauthorised access is attempted.
- Be careful when receiving emails requesting personal information. If you are suspicious do not open the email and report using the Report Phishing icon found in the title bar on Outlook.

10. How can I share and use personal information securely?

I. Postal Service Safe Haven Process

It is recommended that staff members follow these guidelines:

Some examples of documents that may need added protection when sending mail:

- ✓ Birth Certificates
- ✓ Driving Licences
- ✓ Marriage Certificates
- ✓ Passports
- ✓ Bank statements and other financial information.

- Send information that includes personal, commercially confidential or special categories of personal data by ‘Royal Mail Signed For’ or ‘Royal Mail Special Delivery Guaranteed’ or ‘private courier’ but always assess the risk first to determine the most appropriate delivery method. For postage rates and assistance with assessing which method is the most appropriate for the documents see http://www.postoffice.co.uk/mail.
- Ensure that the address is written clearly and in indelible ink and ensure post is sent to a named person or department.
- Clearly mark the top envelope with ‘private and confidential for the addressee only’.
- Include a return to sender address on the back of the envelope.
- Confirm receipt with the intended recipient as early as possible.

The Information Commissioner has issued further guidance regarding the potential for Identity Theft which can be found at ICO guidance on Identity Theft.

II. Paper documents

- Personal and confidential data that is no longer required (e.g. post it notes, messages) should be shredded or disposed of under secure conditions.
- Make a log of what notes have left the department (e.g. home visits etc) and record when they are returned (where appropriate).
- Ensure that documents are properly ‘booked out’ of any relevant filing system if necessary, and records kept of what is sent and where. Copies should be sent or retained, as appropriate.

III. Computers

- Do not share your logons and passwords with anyone.
- PCs or laptops should be locked or switched off when you are away from your desk for any length of time.
- Personal and confidential data must be held on approved organisational mechanisms, including ICB network servers, Teams, SharePoint and OneDrive, not on local hard drives or desk top removable media. Where removable media are used such as laptops or memory-USB sticks, these must be encrypted. OneDrive should only be used for personal information non-work related documents.
- Do not store any ICB owed data on OneDrive, this must only be used to store personal documentation.
- Personal and confidential data must not be saved or copied into any PC or media that is ‘outside the NHS’.

IV. Telephone Calls

- Do not make telephone calls discussing personal or confidential data where you can be overheard.
- When you receive a call, check to ensure you are speaking to the correct person, ring back (where possible) to confirm someone’s identity.

V. **Physical Location and Security**

- Do not allow unauthorised people into areas where personal or confidential data is kept unless supervised. Check peoples ID badges, especially if an unknown person is tailgating you into a secure area.

VI. **Store personal or confidential data information in a locked drawer/filing cabinet.**

- When being transporting they should be placed out of sight in the boot of a car.
- If taken home, they should be stored securely at home in a secure place and should not be left in a car.

VII. **Using N365 SharePoint and Teams.**

- When using SharePoint or Teams please see separate N365 Acceptable Use Policy.

11. What should I do if I become aware of a possible breach of security or confidentiality?

Each member of staff has the responsibility to ensure that information is handled, stored and transferred in a safe, secure and appropriate way. Members of staff should always:

- Report any incident that could possibly relate to a breach of personal, commercially confidential or special categories of personal data, e.g. the loss, theft or corruption of information, a network security breach, loss or theft of a computer, password misuse, etc. following the Incident Reporting Policy.
- Think carefully before sharing personal, commercially confidential or special categories of personal data without explicit consent, as staff will be held accountable for any unauthorised disclosure.
- Report any possible cyber incidents to the IT Team.
- Do not open any suspicious emails, report any suspected phishing/spam using the Phishing Icon mention in previous section
- Under the Data Protection Legislation where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO must be informed no later than 72 hours after the organisation becomes aware of the incident.

If in any doubt, ask your line manager or the SCW Information Governance Team who may pass the query to the DPO, SIRO or the Caldicott Guardian.

The Information Commissioner's Office (ICO) has the power to conduct investigations into breaches of the data protection legislation which can lead to an organisation having an information notice, an assessment notice or an enforcement notice, imposed upon them.

The ICO may impose the penalty notices if the organisation has seriously breached the Data Protection Legislation principles taking the following into account:

a) The nature, gravity and duration of the failure
b) The intentional or negligent character of the failure
c) Any action taken by the Controller or Processor to mitigate the damage or distress suffered by data subjects
d) The degree of responsibility of the Controller or Processor
e) Any relevant previous failures by the Controller or Processor

f) The degree of co-operation with the commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure
g) The categories of personal data affected by the failure
h) The manner in which the infringement became known to the commissioner, including whether, and if so to what extent, the Controller or Processor notified the commissioner of the failure
i) The extent to which the Controller or Processor has complied with previous enforcement notices or penalty notices
j) Adherence to approved codes of conduct or certification mechanisms
k) Any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly)
l) Whether the penalty would be effective, proportionate and dissuasive.

12. How does the ICB ensure staff are using information appropriately?

Staff members should be aware that electronic systems that access, process or transfer data are monitored on a continuous basis. Any breach of security or infringement of confidentiality may be regarded as serious misconduct, which would lead to disciplinary action or dismissal in accordance with disciplinary procedures. In addition, unauthorised disclosure of personal, commercially confidential or special categories of personal data is an offence and could lead to prosecution of individuals and/or the organisation.

13. How should I look after my smartcard?

Smartcards are required to access IT systems essential to healthcare provision. Primary Care Contractors use Smartcards to gain access to patient information i.e. those who provide the Choose and Book service and the Electronic Prescription Service.

Individuals are granted access to a Smartcard by the organisation’s Registration Authority lead. It is up to the Registration Authority Team to verify the identity of all healthcare staff that requires access to personal, commercially confidential or special categories of personal data. Individuals are granted access based on their work and their level of involvement in patient care. The use of Smartcards leaves an audit trail.

Staff should be aware that disciplinary action may be taken if Smartcards are shared or lost.

Line Manager Responsibilities:

- To identify all roles within their area of responsibility which require access to the system and ensure that all employees, including temporary/agency/bank and locum employees, are provided with appropriate access.
- To ensure for all roles that involve access to the system that job descriptions and any recruitment materials make reference to the need to be registered and the role’s responsibilities in relation to using the system.
- To ensure that all new starters within their area of responsibility, including agency/temporary employees, receive training in order to be able to access the system.
- To ensure that all employees are aware of Information Governance policies, associated documentation and their responsibilities in relation to use of and access to the system.
- To immediately inform the Registration Authority Team, of any leavers, starters and staff changes.

Staff Smartcard Code of Practice

- Use your Smartcard responsibly and in line with your access rights.
- Inform the Registration Authority and report an Incident immediately should your Smartcard be lost, stolen or misplaced.
- Ensure that you report any misuse of the Smartcards.
- Ensure that you keep your Smartcard and log-in details confidential. In particular you must not leave your PC logged in and you must not share or provide access to your Smartcard or passwords.
- Ensure that you accurately complete the necessary paperwork, provides suitable identification and attend any appropriate appointments in order to register on the system or have your Smartcard updated/re-issued.
- All members of staff using Smartcards should follow the organisation's suite of Information Governance policies and procedures; adhere to the Data Protection Legislation and Caldicott Principles, the Confidentiality Code of Practice and the Care Records Guarantee.

14. How do we ensure the security of our information and IT systems?

Without effective security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties. Information, whether in paper or electronic form, is of high importance to the ICB, therefore the organisation must ensure that the information is properly protected and is reliably available.

- Access to all ICB data whether held on paper or electronically must be restricted.
- All employees should wear identification badges and should challenge individuals not wearing identification.
- Visitors should be met at reception points and accompanied to appropriate member of staff or meeting.
- Employees on termination of employment or contract must surrender door cards/keys, Identification badge(s) and all relevant ICB equipment in compliance with the leavers process.
- All Information assets including hardware, software and smartcards must be recorded on an asset register that details the description, specification, user and location of the asset.

All staff are responsible for safeguarding against any security breaches occurring as a result of their actions. The organisation will investigate all suspected and actual security breaches.

15. What steps should I take when working at home or outside of the office?

It is important for staff to protect information which is processed outside of the office or is stored on portable devices. Staff are responsible for the security of any portable devices (e.g. Laptops and mobile phones) issued to them and should take all necessary precautions to avoid loss, theft or damage. Staff are also responsible for ensuring no other person can access ICB information of systems. In the event of inappropriate access, loss, damage or theft occurring, they must report this immediately to their line manager. Any loss should be reported on Datix Reporting data breaches - The Hub

When working from home or out of the office there is a need to be vigilant and consider what steps you need to take in order to comply with your Data Protection obligations.

Consider your Working Environment:

- Make sure you consider carefully where you will be working in your home.
- Make sure if you are working with sensitive information, you distance yourself from others in the home. Remember that no one else should see your work information or overhear confidential phone calls.
- You may need to move to a different room to take a confidential phone call or plan to have this type of call at a different time/location.
- It is recommended that you have a conversation with family/household members who may overhear conversation and advise them of confidentiality requirements for which you are responsible.
- Employees working from home should ensure that windows and doors are secured when the property is unoccupied.

Consider your Laptop Security:

- Only use a work provided device for accessing confidential information, encryption is mandatory.
- Ensure that all laptops, records and anything that is valuable to the organisation is kept secure whilst in transit and stored off site.
- Turn the laptop off and log out when it is not in use. Just as you would in the office, ensure that you lock the laptop screen when it is left unattended.
- Any portable computing device must not be left unattended in a public place or left in unattended vehicles either on view or overnight. When transporting it, ensure that it is safely stored out of sight.
- Ensure there are limited opportunities for the laptop to get broken (e.g. spilt drink).
- Consider where you use your laptop and ensure that others cannot view confidential information either within the room or through windows.
- Staff should take extra vigilance if using any portable computing device during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of the organisation’s stored information by a third party “overlooking”. There are security measures which can be deployed to support this if such travel is common to the role, staff should enquire through their line managers.
- Passwords and/or PINs should not be written down, but if unavoidable, should be held on your secure drive in a passwords folder and never kept with the device or in an easily recognised form. Passwords must never be visible in a place where others can access them.

Consider any Paper Records and Post

- If you need paper records these will need to be kept secure and taken home only where necessary and with appropriate approval. It is not appropriate to take home patient records without management approval.

- If you create any confidential waste this needs to be securely destroyed. This must not go into general waste. If possible, destroy with a crosscut shredder as a minimum. If this is not possible, keep securely until such time as you can bring back to the office and securely destroy there.
- If you need to send any letters, where possible send the communication by email instead.
- Avoid getting personal information posted to your home address where at all possible.

16. Can I use Artificial Intelligence (AI) Software?

If you are thinking of using AI software this needs to be discussed with the ICB Digital Team or SCW Information Governance Team before implementation and this may involve the completion of a DPIA or approval or use if the system/app.

17. Can I use a USB memory device?

- Information containing personal, commercially confidential or special categories of personal data must not be stored or transferred using any unencrypted “USB Memory” device.
- Where it is not possible to encrypt data, the advice of the SCW Information Governance Team should be sought and, a one-off data transfer solution should be found using a secure method.
- Portable devices should only be used to transport personal, commercially confidential or special categories of personal data when other more secure methods are not available.
- Information and data should not be stored permanently on portable devices. Always transfer documents back to their normal storage area as soon as possible.
- All staff should be aware of their surroundings when using a mobile device, especially when discussing confidential information.
- Staff must not connect any personal or other devices not issued by ICB to their portable devices.

18. What is Records Management?

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation all the way through to their lifecycle and their eventual disposal. It is a requirement for the ICB to ensure that records are accurate and reliable, can be retrieved swiftly and kept for no longer than necessary.

The NHS has two categories of records: Health and Corporate.

Health records can be considered records which contain the following:

- All patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers, etc.).

Corporate Records can be considered records which contain the following:

- All administrative records (e.g. Personnel, estates, financial and accounting records, notes associated with complaints).

Records within the NHS can be held in paper (manual) or electronic form and as the National Care Record service is now implemented, all NHS organisations will have a duty to ensure that their record systems, policies and procedures comply with the requirements of the Care Record Guarantee.

Corporate Records

Records are the corporate memory of an organisation. Records are a fundamental corporate asset and are required to provide evidence of actions and decisions, enabling the organisation to be accountable and transparent, and comply with legal and regulatory obligations such as the Data Protection Regulations Legislation and the Freedom of Information Act 2000.

Corporate records also support strategic decision making enabling the organisation to protect the interests of staff, patients, public and other stakeholders.

Corporate Records should:

- Be accurate and complete
- Be arranged systematically
- Should be sufficient to enable other members of staff to carry out their tasks
- Should demonstrate compliance with legal and regulatory requirements.

Paper (Manual) Records

- A uniform filing system should be implemented to ensure that documents are grouped appropriately and consistently. Records that are frequently used should be stored within secure filing cabinets or secure areas (locked rooms, coded areas). Infrequently used records should be archived in secure rooms. If records are no longer needed and do not need to be kept according to the retention timeframes, the records should be securely destroyed.
- The filing system should also be kept simple and easy for all to understand.
- It should also be discussed with line management whether records are to be kept manually or electronically. This will help determine the definitive record.
- Paper files should be labelled accurately and clearly. Labels should be brief, have a meaningful description of the contents, and intelligible to both current and future members of staff.
- Where appropriate templates should be used.
- Version controls should be applied and periodically reviewed.
- All paper files should be reviewed at the end of every financial year. This will identify if records need to be retained, archived or destroyed. It would be useful to have a tracker card or spread sheet to include who uses the file, location of where the file is situated and also retention review date.
- Should the file contain personal, commercially confidential or special categories of personal data it is important not to add this to the title of the record and should be kept in a secure location. Page numbering confidential files will confirm if pages have been removed or are missing (if patients records are retained NHS guidance is to include the individuals NHS number).
- Permission to access personal, commercially confidential or special categories of personal data should be restricted to a limited number of staff who requires access.
- Records should be reviewed on a periodic basis to ensure that destruction rules apply, and the necessary steps taken to arrange destructionss that are due..

Electronic Records

- Electronic files should be named accurately, simply and be easy for all to understand. A file structure should be used to ensure that all members of staff can follow the same filing structure.
- It is best to restrict ‘creating or deleting folder responsibility’ to limited number of staff. If all members of staff create files, then there is a possibility of duplication, loss of information and more storage space would be required. Should a member of staff require a new folder to be created, they will need to granted permission from the lead administrator.
- All electronic files should be reviewed at the end of every financial year. This will identify if records need to be retained and archived.
- Each department/directorate should compile a list of standard terms and uniform terminology as naming conventions for files and folders.

- Version controls should be applied and periodically reviewed.
- Records with personal, commercially confidential or special categories of personal data should be controlled using logins, password protection and encryption. Please review the Information Security Policy.

Please refer to the ICB's Records Management Policy. Any queries on Records Management can be directed to bnssg.foi@nhs.net

All staff have a responsibility to review, archive and destroy records – paper or electronic – in line wit the retention schedule in the Records Management Policy

What to do in the Event of Missing Corporate or Health Records

Missing records are a serious risk to the ICB, and it is therefore vital that a tracing procedure is undertaken. Should records go 'missing' the following procedures should be followed:

1. Highlight the fact that a record is 'missing' to the Directorate Lead/Information Asset Owner (IAO) and work colleagues as soon as this becomes apparent.
2. Search in the place you would normally expect to see the record but look either side and above and below where it should be filed (should the record be manual). Search in other folders or conduct a 'search' within your files and folders (should the record be electronic).
3. Should the record remain missing after your search, you will need to contact the SCW Information Governance Team.
4. Relevant staff should be made aware of the name of the record that is missing.
5. The DPO, SIRO (Deputy) and Caldicott Guardian should be informed of the loss and advised of the level of the information risk.
6. Consideration will then be given as to whether the loss needs to be reported to the Information Commissioner's Office.

Inform the Directorate Lead/Information Asset Owner (IAO) and the SCW Information Governance Team if the records have been returned.

Any queries relating to lost records should be directed to the SCW Information Governance Team via the bnssg.data.protection@nhs.net mailbox.

19. What do I need to know about Freedom of Information?

The Freedom of Information Act 2000 (FOIA) encourages transparency within the public sector and assumes that openness is standard so that, for example, decisions on how public money is spent or services provided can be seen and understood. Freedom of Information requests are managed under the Freedom of Information Policy.

How to Identify a Freedom of Information Request

Any member of the public (locally, nationally or globally) can ask to see information that is held by the ICB, and any member of staff may be approached and asked for information under the FOIA.

The law requires BNSSG to respond **within 20 working days** of receipt and staff need, therefore, to be alert to any requests received to ensure they are processed promptly and appropriately.

The FOIA gives a right of access to information and does not require justification or the reason behind the request to be provided by the requestor.

ALL staff have a duty to:

Recognise requests made under FOI:
Enquirers do not have to mention the term FOIA so consider this if the request **does not** fall into one of the following categories:

- A solicitor's letter
- A complaint
- A request for access to personal records
- A press enquiry
- Research
- A routine enquiry which can be responded to as "business as usual" i.e. advice, leaflets, contact details etc.

Provide help and advice to applicants:

- Direct all requests to the Freedom of Information lead for action.
- Advise applicants that the request must be written (email is acceptable) and includes a name and contact address; help them put their request in writing if necessary.
- Direct requesters to the Publication Scheme if it is known the information requested can be sourced there.
- Advise there are several exemptions within the FOIA under which the ICB may not be obliged to provide the information requested.

Action requests for information they hold:
BNSSG is obliged to respond to requests; failure to comply with the FOIA has legal implications not only for the ICB but for each individual member of staff.

Under the FOIA all types of recorded information can be requested and may be disclosed, including everything written in notebooks or on "Post It" notes as well as your formal paper and electronic records. Very little information is "exempt", this is only applicable where the public interest is best served by non-disclosure.

For all FOI questions and queries please email the FOI mailbox.bnssg.foi@nhs.net

21. How does the ICB identify potential impacts to its information?

Business Continuity Management (BCM) is a method used to identify potential impacts that may threaten the operations of the ICB. The fundamental element of business continuity is to ensure that whatever impacts occur the organisation continues to operate.

Business continuity plans (BCP) will help shape organisational resilience to 'threats', plan counteractions and minimise interruptions to ICB activities from the effects of major failures or disruption to its Information Assets (e.g. data, data processing facilities and communications).

Each team should have BCP's in place and it is the responsibility of members of staff to be aware of the location of plans and what procedures to follow in the event of potential 'threats' to the operation of the ICB.

For further information regarding BCP's please contact your line manager.

22. Do I need to complete any training?

Yes. Every individual who works for the organisation is required to complete mandatory annual Data Security and Awareness training and download and read this handbook and the ICBs Acceptable Use Policy accessible through ConsultOD.

This includes all new starters, existing and temporary members of staff and contractors. The ICB has a responsibility to ensure that those working with our information are aware of the Data Protection Legislation principles and the risks to the reputation of the ICB which may occur if processes are not followed**.**

The SCW Information Governance Team have conducted a training needs analysis and identified IG training which will need to be completed by those with additional job roles and functions.

23. How do I know if I can process personal information?

Under Data Protection Legislation certain conditions must be met when processing personal or special categories of personal data. You can contact the SCW Information Governance Team for advice and guidance. They will be able to help you identify whether any of the following conditions can be relied upon:

Conditions for processing personal data	
Article 6, 1 (a)	The Data Subject has given explicit consent
Article 6, 1 (b)	It Is necessary for the performance of a contract to which the data subject is party
Article 6, 1 (c)	It is necessary under a legal obligation to which the Controller is subject
Article 6, 1 (d)	It is necessary to protect the vital interests of the data subject or another natural person
Article 6, 1 (e)	It is necessary for the performance of a task carried out in the public interest or under official authority vested in the Controller
Article 6, 1 (f)	It is necessary for the legitimate interests of the Controller or third party (can only be used in extremely limited circumstances by Public Authorities and must not be used for the performance of the public tasks for which the authority is obligated to do)
Conditions for processing special categories of personal data	
Article 9, 2 (a)	The Data Subject has given explicit consent
Article 9, 2 (b)	For the purposes of employment, social security or social protection
Article 9, 2 (c)	It is necessary to protect the vital interests of the data subject or another natural person where they are physically or legally incapable of giving consent

Article 9, 2 (d)	It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members
Article 9, 2 (e)	The data has been made public by the data subject
Article 9, 2 (f)	For legal claims or courts operating in their judicial category
Article 9, 2 (g)	Substantial public interest
Article 9, 2 (h)	processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (see note below)
Article 9, 2 (i)	processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy
Paragraph 3 of the legislation states that Personal data may be processed for the purposes referred to in point (h) when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies. You must be able to demonstrate this if you are relying on this condition.	

24. How do I record my telephone calls?

The ICB records phone calls in certain departments for the purpose of monitoring the quality of call handling and customer service; facilitating staff training and verifying what was said in case of a dispute or complaint.

Voice recording on telephone extensions in 100 Temple Street must be requested by the line manager/service lead. Line managers must obtain documented approval from the SIRO (Deputy). Requests to the SIRO (Deputy) must include the rationale for the request and the names of individuals who need the facility. Once approval is obtained, this needs to be attached to a request made to IT using TopDesk as indicated on the proforma on the portal. IT will set up the facility and apply a message to callers advising that calls are being recorded.

25. Can I use the chat function within MS Teams meetings?

Yes. The chat function within MS Teams meetings provides a useful way of communicating with meeting attendees and sharing relevant information. You should be aware of the following:

- Chat remains accessible after meeting
- Chat is accessible to everyone within the meeting/team and to anyone who is added at a future date

- Chat should not be used to share confidential or personal information or to share documents
- Please remember that not all individuals can read the chat and reasonable adjustments may be needed to ensure that meetings are inclusive.

26. Can I record a meeting?

Yes, meetings can be recorded but there is a requirement to consider the following:

Consent: there is a need to inform the attendees that the recording /transcribing is taken place and ask if there are any objections.

Retention: Deletion of all recordings/transcriptions is the responsibility of the meeting organiser and any user who records/transcribes a meeting, as a participant. Once the recording is no longer required for business use it should be deleted.

Access: It is the responsibility of all participants who have access to a recording/transcription to ensure any recording/transcription is handled with the same care as any other ICB official information and not shared with parties who are not authorised to see that information.

27. Can I take my laptop and work whilst out of the country?

There are restrictions as to the countries you may be authorised to work due to security risks. Temporary working abroad must be approved by your line manager and an assessment of what systems and information is being access is required. Further information on the approval process and the restrictions can be found in the ICBs Temporary Working from Abroad Policy.

28. Why are some websites blocked and how can I gain access to them?

We block access to websites for a number of reasons such as to protect us from web-borne malware and offensive or inappropriate content. If during the course of your employment you require access to a site that is blocked, you should first discuss this with your line manager. If it is agreed that access is required for a work-related purpose, then a request should be submitted to IT Service Desk.

29. What do I need to do if I want to use a need to do if I want to use a new system or application?

Before any new system or app is used within the ICB it is recommended that you check if a DPIA has been completed and ensure this goes through the Digital Guidance and Approval process which includes a Data Protection Impact Assessment being completed. The system/app should also be added to the Directorate Information Asset Register when approved for use.

A number of systems and apps have been approved for use if the ICB and if you are unsure, please contact the SWC Information Governance Team.

30. Glossary of Abbreviations

Abbreviation	Meaning

BCM	Business Continuity Management
BCP	Business Continuity Plan
BNSSG	Bristol, North Somerset and South Gloucestershire
CSU	Commissioning Support Unit
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Data Sharing Agreement
FOI/FOIA	Freedom of Information Act 2000
UK GDPR	UK General Data Protection Regulations
GP	General Practitioner
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICB	Integrated Care Board
ICO	Information Commissioners Office
IG	Information Governance
SCW	South, Central and West
SIRO	Senior Information Risk Owner

31. Enquiries

Any queries of this document can be sent to bnssg.data.protection@nhs.net