NHS
North East and
North Cumbria

Corporate	ICBP024 Information Security Policy

Version Number	Date Issued	Review Date
V2.1	October 2024	October 2026

Prepared By:	Senior Governance Manager, NECS
Consultation Process:	Integrated Governance Workstream
Formally Approved:	September 2024
Approved By:	Executive Committee

EQUALITY IMPACT ASSESSMENT

Date	Issues
August 2024	None

POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3-year period.

ACCESSIBLE INFORMATION STANDARDS

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact NECSU.Comms@nhs.net

Version Control

Version	Release Date	Author	Update comments
1.0	July 2022	Senior Governance Manager, NECS	First Issue
2.0	October 2022	Senior Governance Manager, NECS	Initial 6 monthly review following ICB establishment, no updates required
2.1	August 2024	Senior Governance Manager, NECS	Natural review date, minor updates made

Approval

Role	Name	Date
Approver	Executive Committee	July 2022
Approver	Executive Committee	October 2022
Approver	Executive Committee	September 2024

Contents

1. Introduction 4
2. Definitions 6
3. Information Security 7
4. Implementation..15
5. Training Implications 16
6. Documentation..16
7. Monitoring, Review and Archiving 16
Schedule of Duties and Responsibilities...18
Appendix A – Equality Impact Assessment 22
Appendix B - Caldicott Principles...25

1. Introduction

The ICB aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the ICB will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

This policy sets out the detailed procedures, rules and standards governing information security that all users of the ICB's information systems must comply with. This policy states the ICB's commitment to information security and sets out the ICB's overall approach to managing information security.

The ICB has a duty to meet legislative and regulatory requirements in relation to information security. These include the NHS Digital Data Security and Protection Toolkit and Statement of Compliance and the legislation, guidance and associated policy documents listed in section 7 of this policy.

It is essential that all the ICB's information systems are protected to an adequate level from business risks. Such risks include accidental data change, loss or release, malicious user damage, fraud, theft, failure and natural disaster. It is important that a consistent approach is maintained to safeguard information in the same way that other more tangible assets are secured, with due regard to the highly sensitive nature of some information held on both electronic and manual systems.

Information security must address both the relevance and the level and type of threats to which information systems and their associated assets are exposed. To ensure that assets are protected against compromise, it is important that this Information Security Policy and associated procedures meet the following objectives;

- deal with the prevailing threats;
- be cost effective;
- add value by reducing the risks to assets;
- be incremental, that is, apply security controls appropriate to the value of the assets involved;
- be just, open and reasonable, where they impinge on the lives of employees;
- be credible and workable, that is, user-friendly, understood, respected and supported by all individuals required to use them
- be cost effective and responsive to the needs of the ICB, and not any more intrusive to on-going business and operations than is necessary;
- reflect the 'need to know' principle.

The security that can be achieved through technical means is limited and needs to be supported by appropriate management controls and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the ICB.

1.1 Status

This policy is an Information Governance policy.

1.2 Purpose and scope

This policy aims to ensure that;

- information systems used in the ICB are properly assessed for security;
- appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information and information systems;
- all staff are aware of their roles and responsibilities for information security;
- a means is established to communicate an awareness of information security issues and their impact on the ICB to management, users and other staff.

It is essential that all information processing systems are protected from events which may jeopardise the activities of the ICB. These events may be accidental as well as behaviour deliberately designed to cause difficulties. Adherence to this policy and related policies and procedures will ensure that the risk of such occurrences is minimised.

This policy will ensure that all information systems, including computer systems, network components and electronically held data, are adequately protected from a range of threats. This policy and associated guidelines cover all aspects of information security from paper-based records to IT systems, administration systems, environmental controls, hardware, software, data and networks.

This policy applies to;

- All staff employed by the ICB, agency workers, contractors, students, trainees, temporary placements who have access to information systems or assets belonging to the ICB.
- Other individuals and agencies who may gain access to data, such as non-executive directors, volunteers, visiting professionals or researchers, and companies providing information services to the ICB.

2. Definitions

The following terms are used in this document:

2.1 **Confidentiality** is defined as the restriction of information and assets to authorised individuals.

2.2 **Integrity** is defined as the maintenance of information systems and physical assets in their complete and proper form.

2.3 **Availability** is defined as the continuous or timely access to information, systems or physical assets by authorised individuals.

2.4 **Encryption** is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.

2.5 **Information Asset** is defined as either personal information, corporate information, computer software, hardware, system or process documentation.

2.6 **Information Asset Owner (IAO)** is the senior individual within the service who is responsible for ensuring that specific information assets are handled and managed appropriately. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the Senior Information Risk Owner (SIRO) on the security and use of those assets.

2.7 **Information Asset Administrators (IAA)** support the IAO to ensure that this procedure is followed, recognise actual and potential security incidents, and consult the appropriate IAO on incident management.

2.8 **Privacy by design** is a concept explained within the General Data Protection Regulations and is about considering data protection and privacy issues upfront in everything we do. It can help ensure compliance with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability. See Article 25 GDPR.

2.9 **Privacy by default** is a concept explained within the General Data Protection Regulations and is about the Controller of personal data implementing appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. See Article 25 GDPR.

2.10 **Removable Media** is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. CDs/DVDs, USB flash memory sticks or pens, PDAs.

2.11 **Smartcard** is a card (like a credit card) with an embedded microchip for storing information. The NHS smartcard is used to control security access to electronic patient records and patient administration systems.

3. Information Security

This policy will be supported by system-specific security policies, technical standards and operational procedures, which will ensure that its requirements are understood and met across the ICB.

3.1 Information Assets

The ICB will ensure that;

- all information assets and personal data flows under its control are identified and documented in an Information Asset Register/Record of Processing Activities in accordance with GDPR;
- all information assets for which IAOs are responsible are reviewed to identify potential threats to the system, and the likelihood of those threats occurring;
- the cost of countermeasures against perceived threats is commensurate with threats to security, the value of the assets being protected and the impact of security failure;
- System Specific Security Policies and Standard Operating Procedures are in place for all systems under their jurisdiction (i.e. the systems they own or are responsible for);
- all staff are fully trained in the use of the systems that they are required to operate;
- staff must not operate systems for which they have not been trained;
- the ICB's electronic information assets are protected from the threat of viruses and other malicious software;
- business continuity plans are in place to protect critical business processes from the effects of major failures of IT systems or other disasters;
- Privacy by design and default are considered at the outset of any new project, system or process involving information assets.

3.2 Computer Hardware & Software

3.2.1 Authorised hardware and software

3.2.1.1 Only hardware approved by the ICB may be used or connected to its network. Any unauthorised hardware found will be removed. Only software approved by the ICB may be used. Unauthorised software must not be used on ICB equipment or on its network. Any unauthorised software found will be removed and may result in disciplinary action.

3.2.1.2 Only authorised staff may install, modify or upgrade hardware or software belonging to, or provided by the ICB.

3.2.1.3 All software licenses must be held by the IT department as this is required for the asset register and also should any reinstall be necessary.

3.2.2 Use of personal equipment

3.2.2.1 Personal equipment must not be used on the ICB's network for the purpose of carrying out organisational business. Encryption controls may impact on the running of personal equipment which in turn may result in permanent damage to the device. The ICB cannot be held liable should any damage to personal equipment occur. This personal equipment may include (but is not exhaustive) PDAs, smart phones, laptops, tablets and external hard drives.

3.2.2.2 Personal equipment or equipment from other organisations could be used on a public network (if/when available) at work premises with appropriate authorisation as this does not provide any access to the organisation's data.

3.2.2.3 Personal equipment (such as laptops, PCs, tablets, and mobile phones must be locked whenever the user is away from their workspace.

3.2.3 Information storage and backup

3.2.3.1 Staff are responsible for ensuring their information is saved appropriately. Where a staff member has network access, all information must be saved to their network drive which is automatically backed up by NECS ICT department.

3.2.3.2 Staff are advised that the authorised encrypted memory stick is only for the transfer of information, not storage of information, and the original content must be saved to the network.

3.2.4 Public Key Infrastructure (PKI) and Secure Socket Layer (SSL)

3.2.4.1 The ICB's network uses digital certificates to provide additional security on the network to provide encryption using PKI algorithms. This approach which works invisibly in the background provides an additional level of security for the network by only allowing authenticated equipment with digital certificates to be a member of the network.

3.2.4.2 Web based organisational databases that contain personal information and are accessed via the web must be secured using Secure Socket Layer (SSL) encryption. e.g. (has https: in the address bar and a padlock icon on the toolbar)

3.2.5 Cloud Computing

3.2.5.1 The Cloud computing concept provides the ability to access data stored within the cloud by many different tools. Examples of Cloud Computing hosting organisations are:

- Google
- Drop Box
- Office 365 (Microsoft)
- Amazon

3.2.5.2 No data belonging to the ICB is to be stored or placed in a Cloud environment without the approval of the IAO and Information Governance service. Some of the issues are listed below (this is not exhaustive);

- Data storage area of the cloud will not normally be known and may be based external to the UK
- Data Storage area could be shared and not segregated from another organisation's data
- No access to data if unavailable due to downtime/system failure

- No contract with the hosting organisation thereby lack of control over the data as the data controller

3.2.6 Internet Protocol (IP) Phones

3.2.6.1 IP phone systems allow telephone calls to be made across an internet connection rather than via standard telephone system IP phones are subject to similar security risks to un-secured email, for example ‘eavesdropping’, ‘traffic sniffing’ and ‘unauthorised re-routing’.

3.2.6.2 The IP Phone systems will transmit and receive data on their own segmented part of the network which is unavailable to other network devices.

3.3 Access Controls

3.3.1 All staff wishing to access the ICB network must firstly accept the user agreement. In doing so, the user agrees to abide by the terms and conditions stated as well as the policies of the ICB.

3.3.2 No one shall be granted access to an information system that does not require that access as part of their work for the ICB. Any access granted is following agreement with the IAO to ensure that access is limited to that required.

3.4 Passwords

3.4.1 The primary form of access control for the ICB computer systems is via password. Each member of staff using a computer system will have an individual password.

3.4.2 Sharing of passwords by both the person who shared the password and the person who received it is an offence under the Computer Misuse Act 1990. All staff must follow robust security practices in the selection and use of passwords.

These will include;

- Logon details are not to be shared or used under supervision even in training situations

- ensuring strong passwords are used i.e. using a minimum 8 digit combination of letters, numbers and special characters (!?£&%$ etc) and to ensure that consecutive passwords are not used e.g. mypassword1, mypassword2, mypassword3 etc.

- not writing down passwords where they can be easily found, i.e. on sticky notes next to their workstation

- ensuring passwords are changed when prompted

- changing their password immediately if they suspect it has been compromised and reporting the incident using the organisation incident reporting system.

- not basing their password on anything that could be easily guessed by another, such as their own name, make of car, car registration, name of pets etc.

- not recycling old passwords

3.5 National Applications Systems Controls

The ICB follows the national Registration Authority Policy; https://digital.nhs.uk/services/registration-authorities-and-smartcards#national-registration-authority-policy which is provided through the ICB's IT provider.

3.5.1 National Spine enabled systems are controlled by a number of different security mechanisms including:

- **Smartcard:** Access will be restricted through use of an NHS Smartcard with a pass code,

- **Training***:* Access to the NHS Care Record Service will only be allowed following appropriate training

- **Legitimate relationships***:* Staff will only be able to access a patient's record if they are involved in that patient's care

- **Role based access control (RBAC)***:* Access will depend on staff roles/job/position functions. Roles and access privileges will be defined centrally and given locally by people designated to do this in the organisation

- **Sealed envelopes:** Patients will be able to hide certain pieces of information from normal view. This will be called a patient's sealed envelope

- **Audit trails***:* Every time someone accesses a patient's record, a note will be made automatically of who, when and what they did

- **Alerts*:*** Alerts will be triggered automatically both to deter misuse of access privileges and to report any misuse when it occurs e.g. if breach of sealed envelope or no legitimate relationship being present.

3.6 Access to other staff members' data

3.6.1 Email

3.6.1.1 In cases where, for example, due to unplanned sickness there is a requirement for access then permission can only be given to the Line Manager to access the account through contact with the IT Service Desk.

3.6.1.2 Staff must ensure they provide access to their Line Manager or other appropriate person in cases of planned absences.

3.6.2 Personal Folders

In cases where there is a requirement for access to data e.g. due to unplanned sickness, then permission must be sought from the folder owner before access can be granted by the IT Service Desk.

3.7 Remote Access and Mobile Working

3.7.1 Staff must not attempt to connect to the ICB's network remotely other than via the agreed remote access solution provided by the IT service.

3.8 Incidents and Risks

3.8.1 All risks and incidents relating to information security must be reported using the ICB's standard procedures for risk and incident reporting.

3.8.2 The reporting of risks and incidents is important to ensure that appropriate action is taken to minimise impact, avoid reoccurrence and to share any lessons learned.

3.8.3 In the case of serious incidents the ICB may have to secure digital forensic evidence, for example, on a hard drive to prevent this from being tampered with during formal disputes or legal proceedings.

3.9 Internet and Email Security

3.9.1 When accessing the Internet or email the following must be adhered to;

- Before using the Internet, Intranet or email for the first time all staff must accept the terms and conditions of the user code of connection.

- No illicit or illegal material may be viewed/downloaded or obtained via the Internet or email.

- Any material downloaded must be virus checked automatically by the system's anti-virus system.

- The user will make their system available at any time for audit either by the IT department or internal and external audit.

- Be mindful of cyber security and do not click links within emails from unknown or untrustworthy sources.

3.9.2 Usage is monitored by the ICB and any breaches of security, abuse of service or non-compliance with the NHS Code of Connection or organisational policy may result in disciplinary action, as well as the temporary or permanent withdrawal of all N3 services including email.

Further information is available in the Email and Internet Acceptable Use Policy

3.10 Transferring information and equipment

3.10.1 It is imperative that the utmost care is exercised when transferring information, especially information of a confidential nature e.g. staff, patient or service user information. This includes transferring information by telephone (voice and text), email, courier and public mail.

3.10.2 Caldicott principles must be followed at all times where patient/person-identifiable information is concerned. A 'Caldicott 2' review was published in March 2013 which amended the Caldicott Principles, and a further review in 2020 which added an eighth principle, which are listed in Appendix B.

3.10.3 Regular exchanges of personal information must be governed by information sharing protocols or data processing agreements within contracts.

3.10.4 Staff must not leave any property belonging to the ICB, including laptops, portable devices, mobile telephones, records or files in unattended cars or in easily accessible areas for extended periods, including overnight. These must either be secured within premises under the ICB's control, or where this is not practicable secured within the employee's home. Where an overnight stay for work purposes is required, the same principles apply.

3.10.5 In instances where equipment or records are unavoidably left unattended for short periods e.g. calling at another base, making an unscheduled stop, the staff member must assess the potential risk to the equipment whilst it is unattended. A formal written risk assessment need not be undertaken but the staff member must make a judgement on the security of the equipment.

3.10.6 If a staff member is required to change their office base, they must not move any IT or telephone equipment. All IT and telephone equipment must be moved by a member of the IT department.

3.10.7 All IT or telephone equipment intended for destruction must be securely disposed of by the IT department in accordance with agreed procedures in place at that time. Destruction certificates will be obtained and held by the IT department.

3.11 Systems Development, Maintenance & Security

3.11.1 The ICB must ensure that security requirements are built into systems from the outset. Suitable controls must be in place to manage the purchase or development of new systems and the enhancement of existing systems, to ensure that information security is not compromised.

3.11.2 IAO and IAA implementing or modifying systems are responsible, in collaboration with the CSU ICT service for ensuring;

- the Computer Misuse Act warning is displayed on all organisation equipment prior to logging on to the network
- that all modifications to systems are logged and up to date documentation exists for their systems and follow change control procedures
- contracts with suppliers must include appropriate information security and confidentiality clauses

- they complete a risk assessment in liaison with the CSU ICT service

- that vendor supplied software used in systems, is maintained at a level supported by the supplier, if beneficial to the service. Any decision to upgrade must take into account the security of the release e.g. software drivers that come with printers to operate the printer, and clinical safety

- that physical or logical access is only provided to suppliers for support purposes when necessary, and must be with IAO and ICT approval

- that all supplier activity on the system is monitored

- that copies of data must retain the same levels of security and access controls as the original data

3.11.3 A Data Protection Impact Assessment must be completed prior to installation, in liaison with the Information Governance Team, to ensure all information security aspects of new and modified systems are considered and risk assessed.

3.12 Business Continuity Plans

3.12.1 The ICB must have a Business Continuity Plan that allows critical systems within each service area to be maintained and to restore critical systems in the event of a major disruption to systems e.g. through a disaster or security failure. This supports the wider organisation business continuity planning. The CSU provides ICT services to the ICB and has its own Business Continuity Plan.

3.12.2 It is the responsibility of the IAOs to ensure that their sections of the ICB business continuity plans are regularly updated to reflect changes in service delivery.

3.12.3 Business continuity plans should be tested annually to ensure they work. The responsibility to co-ordinate the exercises will lie with individual IAOs.

4. Implementation

4.1 This policy will be available to all staff for use in relation to the specific function of the policy and for use in the circumstances described within section 1.

4.2 All directors and managers are responsible for ensuring that relevant staff within their own directorates and departments have read and understood

this document and are competent to carry out their duties in accordance with the procedures described.

5. Training Implications

It has been determined that there are no specific training requirements associated with this policy/procedure. However staff are required to complete induction training which includes IT security and to complete mandatory Data Security Awareness training annually.

6. Documentation

6.1 Other related policy documents.

- Confidentiality and Data Protection Policy
- Information Governance and Information Risk Policy
- Internet and Email Acceptable Use Policy

6.2 Legislation and statutory requirements

- Cabinet Office. (2018) *Data Protection Act 2018*. London: HMSO
- Cabinet Office. (1998) *Human Rights Act 1998*. London: HMSO
- Cabinet Office. (1990) *The Computer Misuse Act 1990*. London: HMSO
- Cabinet Office. (2000) *The Electronic Communications Act 2000*. London: HMSO
- General Data Protection Regulations (2016)

6.3 Best practice recommendations

- Department of Health, NHS Code of Practice: Information Security http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Informationsecurity/index.htm
- BS ISO/IEC 17799:2005 (Information technology -- Code of practice for information security management)
- BS ISO/IEC 27001:2005(Information technology - information security management systems)
- BS7799-2:2005BS7799-2:2005 (Information security management)
- NHS Digital Data Security and Protection Toolkit: https://www.dsptoolkit.nhs.uk/

7. Monitoring, Review and Archiving

7.1 Monitoring

The ICB Board will agree with the sponsoring director a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

7.2 Review

7.2.1 The ICB Board will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

7.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Executive director will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

7.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the Executive director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process

7.3 Archiving

The ICB Board will ensure that archived copies of superseded policy documents are retained in accordance with the NHS Records Management Code of Practice.

Schedule of Duties and Responsibilities

Through day to day work, employees are in the best position to recognise any specific fraud risks within their own areas of responsibility. They also have a duty to ensure that those risks, however large or small, are identified and eliminated. Where it is believed fraud, bribery or corruption could occur, or has occurred, this should be reported to the Counter Fraud Authority or the Executive Director of Finance immediately.

ICB Board	The ICB Board has responsibility for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Chief Executive	The Chief Executive has overall responsibility for the strategic direction and operational management, including ensuring that ICB process documents comply with all legal, statutory and good practice guidance requirements.
Senior Governance Manager, NECS	The Senior Governance Manager will update this policy in line with legislation, guidance and best practice.
Senior Information Risk Owner (SIRO)	The SIRO is responsible for; • Ensuring that an overall culture exists that values and protects information within the organisation. • Owning the organisation's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used. • Advising the Chief Executive on the information risk aspects of their statement on internal control. • Owning the organisation's information incident management framework.

Information Governance Team NECS	The Information Governance Team will; • Provide information governance advice and support for all staff to ensure they are aware of their responsibilities with regard to information security and confidentiality. • Monitor that staff are aware of these responsibilities. • Assist in the investigation of any incidents and development of action plans that occur as a result of failure to comply with this policy.
Caldicott Guardian	The Caldicott Guardian is responsible for; • Representing and championing confidentiality requirements and issues at ICB Board level and, where appropriate, at a range of levels within the organisation's overall governance framework. • Supporting work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required. With support from the Information Governance team, the Caldicott Guardian will: • Ensure the data protection work programme is successfully co-ordinated and implemented. • Ensure the organisation complies with the principles contained within the Confidentiality: NHS Code of Practice and that staff are made aware of individual responsibilities through policy, procedure and training. • Provide routine reports on Confidentiality and Data Protection issues.

Information Asset Owners (IAOs)	IAOs, with the assistance of Information Asset Administrators (IAAs) where necessary will; • Ensure that the system is used within the terms of the ICB Notification with the Information Commissioner and the requirements of both Data Protection legislation and the relevant Code of Practice, paying particular attention to the data protection principles as specified in the Act. Note: the requirement to notify is not in UKGDPR. When developing a new process, or changing an existing process, complete an information governance checklist. This will help to ensure any issues are highlighted and dealt with at an early stage. • Participate in a Data Protection Impact Assessment when commencing a new project which involves personal information. • Restrict the use of the system where appropriate to those authorised users who need access to it for organisational or other authorised work. • Restrict the access to particular sets of personal data available from the system to those authorised users who need access to them for organisational or other authorised work. • Maintain appropriate security measures for the system and any personal data held within it to avoid loss of the personal data or unauthorised disclosure of the personal data. Ensure that all copies of personal data output, or obtained, from the system, whether recorded on paper, computer readable media or any other form, are securely destroyed or erased when they are no longer required for organisational purposes. • Ensure that personal data held in the system are as accurate as possible and kept up to date where relevant and that the department has an effective policy for erasing or deleting and removing personal data as soon as they are no longer required for organisational purposes. • Ensure that all authorised users of the system containing personal data have been properly trained and advised of the organisation's requirements in respect of data protection. • Ensure that personal data is not removed from the organisation premises except where specifically required for the execution of the legitimate functions of the organisation, and with the express permission of the employee's Line Manager. Advice should be sought from the Caldicott Guardian or Information Governance team. • Ensure that the Information Governance team is advised as soon as possible of any incidents or complaints that need to be recorded in the incident reporting system.

Commissioning Support Staff.	Whilst working on behalf of the ICB NECS staff will be expected to comply with all policies, procedures and expected standards of behaviour within the ICB, however they will continue to be governed by all policies and procedures of their employing organisation.
All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.

Appendix A – Equality Impact Assessment

Equality Impact Assessment
Initial Screening Assessment (STEP 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership).

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Liane Cotterill
Job Title: Senior Governance Manager
Organisation: North of England Commissioning Support Unit

Title of the service/project or policy: Information Security Policy

Is this a;
Strategy / Policy ☒ **Service Review** ☐ **Project** ☐
Other Click here to enter text.

What are the aim(s) and objectives of the service, project or policy:
This policy aims to ensure that information systems used in the ICB are properly assessed for security and that appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information and information systems.

Who will the project/service /policy / decision impact?
(Consider the actual and potential impact)

- **Staff** ☒
- **Service User / Patients** ☐
- **Other Public Sector Organisations**☐

- **Voluntary / Community groups / Trade Unions** ☐
- **Others, please specify** Click here to enter text.

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	☐	☒
Has there been or likely to be any staff/patient/public concerns?	☐	☒
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	☐	☒
Could this piece of work affect the workforce or employment practices?	☐	☒
Does the piece of work involve or have a negative impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community	☐	☒

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

The policy is based on legislation and good practice, no impacts identified.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	☒	☐
Please provide the following caveat at the start of any written documentation: **"If you require this document in an alternative format such as easy read, large text, braille or an alternative language please contact (ENTER CONTACT DETAILS HERE)"**		
If any of the above have not been implemented, please state the reason: Click here to enter text.		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Executive Committee	Approver	

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

If you are not completing 'STEP 2 - Equality Impact Assessment' this screening document will need to be approved and published alongside your documentation.

Please send a copy of this screening documentation to: NECSU.Equality@nhs.net for audit purposes.

Appendix B - Caldicott Principles

1. **Justify the purpose(s)**
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data**
   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis**
   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities**
   Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law**
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

8. **Inform patients and service users about how their confidential information is used** A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.