NHS
South Tyneside
Clinical Commissioning Group

Information Security Policy

Ratified	Approved
Status	Final
Issued	December 2020
Approved By	Executive Committee
Consultation	CCG IG Lead NECS IG Team
Equality Impact Assessment	Completed
Distribution	All CCG Staff
Date Amended following initial ratification	September 2020
Implementation Date	December 2020
Planned Review Date	December 2022
Version	6
Author	Senior Governance Officer (IG), NHS North of England Commissioning Support Unit
Reference No	IG05

Policy Validity Statement
This policy is due for review on the date shown above. After this date, policy and process documents may become invalid.

Policy users should ensure that they are consulting the currently valid version of the documentation.

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 stynccg.enquiries@nhs.net

Version Control

Version	Author	Update comments
V1.0	Senior Governance Manager, NECS	Policy adopted by Clinical Commissioning Group (CCG) as part of policy suite developed by NECS
V2.0	Senior Governance Manager, NECS	Policy ratified by Governing Body
V3.0	Senior Governance Manager, NECS	Equality Impact Assessment. Re-formatted to CCG policy standard.
V4.0	Senior Governance Manager, NECS	Review and update: - Reformatted numbering and style of policy. - Table of Contents updated, in reflection of amendments. - Section 8.6: Removal of 'within the service who is responsible for the provision of service' and insertion of ' within the service who is allocated responsibility for the information in their area of work'. - Section 8.10: New paragraph 'Cyber Security is a term that refers to the management and application of Information Security standards. This is typically applied to computers, computer networks, and the data stored and transmitted over them. This can also cover physical security. It is distinct from information governance (IG), which is about the maintenance of the confidentiality of information, especially person identifiable information and medical records'. - Section: 9.3.7.1: New paragraph 'Cyber Security: There is a rising risk of cyber threat across all sectors. The Health and Social Care Information Centre (HSCIC) has been commissioned by the Department of Health to develop a Care Computer Emergency Response Team (CareCERT). CareCERT will offer intelligence, advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats. Section: 9.3.7.2: New paragraph; 'The service will enable a coordinated approach to be taken across the health and social care system, by informing organisations about cyber security vulnerabilities, mitigating risks, and reacting to cyber security threats and attacks. The CCG will be informed via the CSU Technical Security Manager who has been formally registered in the HSCIC CareCERT contact database'. - Section 9.9.1: Insertion of 'These procedures include reporting of cyber security incidents in line with the HSCIC's Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation –

		February 2015'. - Section 9.12.2; Bullet 4: Insertion of 'they complete a risk assessment in the form of a Privacy Impact Assessment in liaison with the CSU ICT service. Guidance on completing a PIA is at Appendix B'. - Section 10: Updated Technical Security Manager (CSU) duties and responsibilities 'The Technical Security Manager (CSU) will; • Provide technical security advice and support for all staff to ensure they are aware of their responsibilities with regard to technical security. • Notify the CCG of any cyber security alerts via the HSCIC's CareCERT process. • Assist in the investigation of any incidents and development of action plans that occur as a result of failure to comply with this policy' - Section 13.1: Insertion of 'HSCIC - Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation – February 2015'. - Insertion of Appendix B; 'Privacy Impact Assessments (PIAs) Guidance'
V4.1	Senior Governance Manager, NECS	Review and update to include GDPR.
V5	Senior Governance Officer (IG), NECS	Revised following publication of the Data Protection Act 2018
V6	Senior Governance Officer (IG), NECS	Reviewed in line with policy requirements

Approval

Role	Name	Date
Approval	Governing Body	24 October 2013 (1)
Approval	Executive Committee	14 January 2015 (2)
Approval	Executive Committee	21 January 2016 (3)
Approval	Executive Committee	January 2018 (4)
Approval	Executive Committee	October 2018 (5)
Approval	Executive Committee	December 2020 (6)

Contents

1. Introduction

The CCG aspire 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 CCG will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

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

The CCG has a duty to meet legislative and regulatory requirements in relation to information security. These include the NHS Digital Data Protection and Security 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 of the CCG'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 kind 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 security policy and 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 CCG, 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 CCG.

1.1 Status

This policy is an Information Governance policy.

1.2 Purpose and scope

1.2.1 This policy aims to ensure that;

- information systems used in the CCG 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 CCG to management, users and other staff.

1.2.2 It is essential that all information processing systems are protected from events which may jeopardise the activities of the CCG. 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.

1.2.3 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.

1.2.4 This policy applies to;

- All staff employed by the CCG, agency workers, contractors, students, trainees, temporary placements who have access to information systems or assets belonging to the CCG.
- 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 CCG.

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 data implementing appropriate technical and organisational measures ensuring 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 CCG.

3.1 Information Assets

The CCG will ensure that;

- all information assets under its control are identified and documented in an Information Asset Register 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 CCG'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

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

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

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

Personal equipment must not be used on the CCG'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 CCG 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.

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.

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

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.

Staff are advised that the authorised encrypted memory stick is only for the transfer of information and the original content must be saved to the network.

3.2.4 Public Key Infrastructure (PKI) and SSL

The CCG'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.

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

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

No data belonging to the CCG 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

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'.

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 CCG 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 CCG.

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 CCG. 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 CCG 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 CCG follow the national Registration Authority Policy https://digital.nhs.uk/services/registration-authorities-and-smartcards#national-registration-authority-policy which is provided through the CCG'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 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

367.1 Email

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.

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 CCG'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 CCG'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 CCG 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 CCG 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.

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, fax, courier and public mail.

3.10.2 Caldicott principles must be followed at all times where patient/person-identifiable information is concerned. These were revised following the Caldicott2 review in March 2013 and are listed in Appendix A.

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 CCG, 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 CCG'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 CCG 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 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

3.12.3 A Privacy 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 CCG 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.

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

3.12.3 Business continuity plans should be tested annually to ensure it works. 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 the circumstances described within section 1.

4.2 All managers are responsible for ensuring that relevant staff within the CCG have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

5. Training Implications

The sponsoring manager will ensure that the necessary training or education needs and methods required to implement the policy or procedure(s) are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

The training required to comply with this policy are:

- IT security training included in induction training for new staff
- Information governance training completed on an annual basis
- Any training necessary to enable staff to operate IT systems safely and securely

6. Related Documents

6.1 <u>Legislation and statutory requirements</u>

- 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)

6.2 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 Connecting for Health Information Governance Toolkit: https://nww.igt.connectingforhealth.nhs.uk/

6.3 Related Policies

- Internet and Email Acceptable Use Policy

7. Monitoring, review and archiving

7.1 Monitoring

The governing body will agree 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 Governing Body 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 governing body 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 second page of this document.

Note: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor 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 Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with the Department of Health's Records Management Code of Practice for Health & Social Care 2016

8. Equality analysis

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 (NECS)

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

Is this a;
Strategy / Policy ☒ **Service Review** ☐ **Project** ☐
Other N/A

What are the aim(s) and objectives of the service, project or policy:
This policy aims to ensure that information systems used in the CCG 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** N/A

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 the CCG's former Information Security policy. There is no fundamental change to the content therefore the previous EIA which concluded 'no impact' remains appropriate.

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	☒	☐
If any of the above have not been implemented, please state the reason: Not applicable		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Executive Committee	Approval	December 2020

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.

Appendix A

Duties and Responsibilities

Governing Body	The Governing Body (GB) 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 Officer	The chief officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.
Information Governance Team (NECS)	The Information Governance Team (CSU), 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 Governing Body 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. • Complete the Confidentiality and Data Protection Assurance component of the Information Governance Toolkit, contributing to the annual assessment. • Provide routine reports on Confidentiality and Data Protection issues.
Technical Security Manager (CSU)	The Technical Security Manager (CSU) will; • Provide technical security advice and support for all staff to ensure they are aware of their responsibilities with regard to technical security • Notify the CCG of any cyber security alerts via the HSCIC's CareCERT process • Assist in the investigation of any incidents and development of action plans that occur as a result of failure to comply with this policy.

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 Officer on the information risk aspects of their statement on internal control. • Owning the organisation's information incident management framework.
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 CCG 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 GDPR/UK Data Protection Bill. • 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 Privacy 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, microfilm, 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.
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 B

Caldicott2 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.