Newcastle Gateshead
Clinical Commissioning Group

Corporate	CCG: IG05: Information Security

Version Number	Date Issued	Review Date
V4	July 2018	July 2020

Prepared By:	Senior Governance Officer (IG), NECS
Consultation Process:	CCG Head of Corporate Affairs CCG Quality, Safety & Risk Committee NECS IG Team

Policy Adopted From:	V4 IG05: Information Security
Approval Given By:	Quality, Safety and Risk Committee
Formally Approved:	5 July 2018

Document History

Version	Date	Significant Changes
1	28/02/2013	First issue
2	14/05/2014	Equality Impact Assessment. Re-formatted to CCG policy standard
3	11/11/15	• Reformatted numbering and style of policy. • Section 4.10: 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: 5.3.7.1: 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. The service will enable a coordinated approach to be taken across the health and social care system, by informing organisations about cyber

		• mitigating risks, and reacting to cyber security threats and attacks. The CCG will be informed via the NECS Technical Security Manager who has been formally registered in the HSCIC CareCERT contact database'. • Section 5.9.1: 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 5.12.2: Insertion of 'they complete a risk assessment in the form of a Privacy Impact Assessment in liaison with the NECS ICT service. Guidance on completing a PIA is at Appendix B'. • Section 6: Updated Technical Security Manager (NECS) duties and responsibilities 'The Technical Security Manager (NECS) 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 9.1: 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'
3.1	October 2017	Review and update to include GDPR
V4	May 2018	Revised following publication of the Data Protection Act 2018 and General Data Protection Regulations 2016.

Equality Impact Assessment

Date	Issues
June 2018	See Section 11 of this document

Policy Validity Statement
This policy is due for review on the latest 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.

Contents

1. Introduction

The CCG 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 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 13 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

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.

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.

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 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 the provision of service. 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 if data implementing appropriate technical and organisational measures to 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.

2.12 **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 personal identifiable information and medical records.

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

- all information assets under its control are identified and documented in an Information Asset Register in accordance with GDPR;

- all information assets for which they 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

3.2.1.1 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.

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

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 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.

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 CSU ICT Department.

3.2.3.2 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

3.2.4.1 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.

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 CCG is to be stored or placed in a Cloud environment without the consent of the IAO and Information Governance. 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.

3.2.7 Cyber Security

3.2.7.1 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.

3.2.7.2 The service will enable a co-ordinated approach to be taken across the health and social care system, by information organisations about cyber security vulnerabilities, mitigating risks and reacting to cyber security threats and attacks. The CCG will be informed by the CSU Technical Security Manager who has been formally registered in the HSCIC CareCERT contact database.

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

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, provided by the local CSU Registration Authority service

- **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

3.6.1 E-mail

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

3.6.2.1 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. 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.

3.8.2 The reporting of risks and incidents is important to ensure that appropriate action is taken to minimise impact, avoid recurrence 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.

- 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 the form of a Privacy Impact Assessment in liaison with the CSU ICT service. Guidance on completing a PIA is at Appendix B.
- 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

- 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 Business continuity plans must exist for each service that allow critical systems 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 individual 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. Duties and Responsibilities

Governing Body	The Commissioning Forum has delegated responsibility to 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.
The Information Governance Team(CSU)	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.

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.
Caldicott Guardian	The Caldicott Guardian is responsible for; • Representing and championing confidentiality requirements and issues at 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. • 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.

Information Asset Owners (IAO)	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.

5. Implementation

5.1 This policy will be available to all staff.

5.2 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.

6. Training Implications

6.1 The Sponsoring Director 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.

6.2 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

7. Related Documents

7.1 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
- HSCIC – Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation – February 2015.
- General Data Protection Regulation (2016)

7.2 Best practice recommendations

- Department of Health, NHS Code of Practice: Information Security http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Informat ionsecurity/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/

7.3 Related Policies

- Internet and Email Acceptable Use Policy

8. Monitoring, Review and Archiving

8.1 Monitoring

8.1.1 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.

8.2 Review

8.2.1 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.

8.2.2 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.

8.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'version control' table on the second page of this document.

NB: 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.

8.3 Archiving

8.3.1 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 and social care 2016.

9. Equality Analysis

An equality impact assessment has been completed:

Partners in improving local health

North of England Commissioning Support

Introduction - Equality Impact Assessment

An Equality Impact Assessment (EIA) is a process of analysing a new or existing service, policy or process. The aim is to identify what is the (likely) effect of implementation for different groups within the community (including patients, public and staff).

We need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not

This is the law. In simple terms it means thinking about how some people might be excluded from what we are offering.

The way in which we organise things, or the assumptions we make, may mean that they cannot join in or if they do, it will not really work for them.

It's good practice to think of all reasons why people may be excluded, not just the ones covered by the law. Think about people who may be suffering from socio-economic deprivation or the challenges facing carers for example.

This will not only ensure legal compliance, but also help to ensure that services best support the healthcare needs of the local population.

Think of it as simply providing great customer service to everyone.

As a manager or someone who is involved in a service, policy, or process development, you are required to complete an Equality Impact Assessment using this toolkit.

Policy	A written statement of intent describing the broad approach or course of action the Trust is taking with a particular service or issue.
Service	A system or organisation that provides for a public need.
Process	Any of a group of related actions contributing to a larger action.

STEP 1 - EVIDENCE GATHERING

Name of person completing EIA:	**Senior Governance Officer, NECS**
Title of service/policy/process:	**Information Security Policy**
Existing: √ **New/proposed:** □ **Changed:**	
What are the intended outcomes of this policy/service/process? Include outline of objectives and aims	
This policy aims to ensure that; **information systems used in the CCGs 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 CCGs to management, users and other staff.** **The policy compliments other Information Governance policies.**	

Who will be affected by this policy/service /process? (please tick)

□ **Consultants** □ **Nurses** □ **Doctors**
√ **Staff members** □ **Patients** □ **Public**
□ **Other**

If other please state:

What is your source of feedback/existing evidence? (please tick)

□ **National Reports** □ **Internal Audits**
□ **Patient Surveys** □ **Staff Surveys** □ **Complaints/Incidents**
□ **Focus Groups** □ **Stakeholder groups** √**Previous EIAs**
□ **Other**

If other please state:

Evidence	**What does it tell me? (about the existing service/policy/process? Is there anything suggest there may be challenges when designing something new?)**
National Reports	**N/A**
Patient Surveys	**N/A**
Staff Surveys	**N/A**
Complaints and Incidents	**N/A**
Results of consultations with different stakeholder groups – staff/local community groups	**N/A**
Focus Groups	**N/A**
Other evidence (please describe)	**N/A**

STEP 2 - IMPACT ASSESSMENT

What impact will the new policy/system/process have on the following: (Please refer to the 'EIA Impact Questions to Ask' document for reference)

Age A person belonging to a particular age

No impact identified

Disability A person who has a physical or mental impairment, which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities

No impact identified

Gender reassignment (including transgender) Medical term for what transgender people often call gender-confirmation surgery; surgery to bring the primary and secondary sex characteristics of a transgender person's body into alignment with his or her internal self perception.

No impact identified

Marriage and civil partnership Marriage is defined as a union of a man and a woman (or, in some jurisdictions, two people of the same sex) as partners in a relationship. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. Civil partners must be treated the same as married couples on a wide range of legal matters

No impact identified

Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context.

No impact identified

Race It refers to a group of people defined by their race, colour, and nationality, ethnic or national origins, including travelling communities.

No impact identified

Religion or belief Religion is defined as a particular system of faith and worship but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.
No impact identified
Sex/Gender A man or a woman.
No impact identified
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes
No impact identified
Carers A family member or paid helper who regularly looks after a child or a sick, elderly, or disabled person
No impact identified
Other identified groups such as deprived socio-economic groups, substance/alcohol abuse and sex workers
No impact identified

STEP 3 - ENGAGEMENT AND INVOLVEMENT

How have you engaged stakeholders in testing the policy or process proposals including the impact on protected characteristics?
No engagement undertaken as this policy has received minor amendments only
Please list the stakeholders engaged:

STEP 4 - METHODS OF COMMUNICATION

What methods of communication do you plan to use to inform service users of the policy?
□ **Verbal – stakeholder groups/meetings** □ **Verbal - Telephone** □ **Written – Letter** □ **Written – Leaflets/guidance booklets** □ **Email** √ **Internet** □ **Other**
If other please state:

ACCESSIBLE INFORMATION STANDARD

The Accessible Information Standard directs and defines a specific, consistent approach to identifying, recording, flagging, sharing and meeting the information and communication support needs of service users.

Tick to confirm you have you considered an agreed process for:
√ **Sending out correspondence in alternative formats.** √ **Sending out correspondence in alternative languages.** √ **Producing / obtaining information in alternative formats.** √ **Arranging / booking professional communication support.** √ **Booking / arranging longer appointments for patients / service users with communication needs.**
If any of the above have not been considered, please state the reason:

STEP 5 - SUMMARY OF POTENTIAL CHALLENGES

Having considered the potential impact on the people accessing the service, policy or process please summarise the areas have been identified as needing action to avoid discrimination.

Potential Challenge	What problems/issues may this cause?
1 None identified.	

STEP 6- ACTION PLAN

Ref no.	Potential Challenge/ Negative Impact	Protected Group Impacted (Age, Race etc)	Action(s) required	Expected Outcome	Owner	Timescale/ Completion date
	None identified.					

Ref no.	Who have you consulted with for a solution? (users, other services, etc)	Person/ People to inform	How will you monitor and review whether the action is effective?
	Non-applicable		

SIGN OFF

Completed by:	**Alan Clement, Senior Governance Officer**
Date:	**June 2018**
Presented to: (appropriate committee)	**Quality, Safety and Risk Committee**
Publication date:	**July 2018**

Appendix A

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.

Appendix B

Privacy Impact Assessments (PIAs) - Guidance

1. Introduction

Privacy impact assessments (PIAs) are a tool which can help the CCG identify the most effective way to comply with its data protection obligations. In addition, PIAs will allow the CCG to meet individuals' expectations of privacy.

An effective PIA will allow the CCG to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

PIAs should be used for new projects or processes and also when projects, processes or services are to be reviewed. Where 'yes'' is the answer to any PIA screening questions (to be found at Annex 1), a PIA should be completed and sent to the Information Governance Team (necsu.ig@nhs.net) for consideration.

2. Background

In February 2014, the Information Commissioner issued a code of practice under Section 51 of the Data Protection Act (DPA) in pursuance of his duty to promote good practice. The DPA says good practice includes, but is not limited to, compliance with the requirements of the Act. Conducting a PIA is not a requirement of the Act, but undertaking one will help to ensure that a new project is compliant. This document is based on the good practice identified in the ICO guidance.

3. What is a PIA?

A privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective PIA will be used throughout the development and implementation of a project, using existing project management processes.

A PIA will enable the CCG to systematically and thoroughly analyse how a particular project or system will affect the privacy of individuals involved.

4. What do we mean by privacy?

Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:

- **Physical privacy** – the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

- **Informational privacy** – the ability of a person to control, edit, manage and delete information about themselves and to decide how to and what extent such information is communicated to others. Intrusion can come in the form of a collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of the messages.

This guidance is concerned primarily with informational privacy.

Privacy risk is the risk of harm arising through an instruction into privacy. This guidance is concerned primarily with the minimising of the risk of informational privacy. Some of the ways risk can arise is through personal information being:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely

The outcome of a PIA should be a minimisation of privacy risk.

5. Projects which might require a PIA

The core principles of PIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

A PIA is suitable within the CCG for a variety of situations:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public), or the application of new technology to an existing system (for example adding Automatic number place recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies, which impact on privacy through the collection of use of information, or through surveillance or other monitoring.

All CCG projects should include a PIA at the outset of the project which will help to reduce the associated costs, avoid costly fixes after the project has started and damage to reputation which might otherwise occur. This should be built into the project management tool in use within the organisation and form an intrinsic part of any project.

6. Dissemination and implementation

The guidance will be communicated to all staff and stakeholders by the most appropriate means.

The implementation of this guidance is achieved through the embedding of the PIA in the project management system. Directors and senior leads will be responsible for ensuring the guidance is implemented in their areas of responsibility and compliance with this guidance may be monitored through the project management tool.

7. Accountability, responsibilities and training

Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

Overall responsibility for the guidance lies with the Information Governance Service (CSU) who have responsibility for managing the development and implementation of information governance procedural documents.

Training and education are key to the successful implementation of this guidance and embedding a culture of information governance management in the organisation.

8. Review

This guidance will be updated at regularly and in accordance with the following as and when required:

- legislative changes
- good practice guidance;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

This guidance will be received by the relevant CCG Committee for approval.

9. Help and Support with this Guidance

Please contact the IG team if you have any queries or questions on this guidance. The IG team can be contacted on:

Email: necsu.ig@nhs.net

The ICO PIA Code of Practice can be found here http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

Annex One

Privacy impact assessment screening questions

These questions are intended to help staff within the CCG to decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA should be undertaken.

1. Will the project involve the collection of new information about individuals?

2. Will the project compel individuals to provide information about themselves

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

6. Will the project result in you making decisions or taking action against individual in ways which can have a significant impact on them?

7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

8. Will the project require you to contact individuals in ways which they may find intrusive?

Annex Two

Privacy impact assessment template

Step One: Identify the Need for a PIA

Explain what the project aims to achieve, what the benefits will be to the CCG, to individuals and to other parties.

You could link this to the original project proposal.

If you decide that your project needs a PIA, explain here what lead you to this conclusion (this could be derived from the 8 questions in Annex One).

Step Two: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation Requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultations? You should link this to the relevant stages of the CCG project management process.

Consultation can be used at any stage of the PIA process.

Step Three: identify the privacy and related risks Identify the key privacy risk and the associated compliance and corporate risks. It may be worth recording this information on the CCG Information Risk Register. Annex three can be used to help identify the Data Protection Act related compliance risks.			
Privacy Issue	Risk to Individuals	Compliance Risk	Associated CCG / corporate risk

Step Four: identify privacy solutions Describe the actions you could take to reduce the risks, and any further steps which would be necessary (e.g. the production of new guidance or future security testing for systems).			
Risk	Solution (s)	Result: is the risk eliminated, reduced, or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step Five: Sign off and record the PIA outcome Who has approved the privacy risks involved in the project? What solution needs to be implemented?		
Risk	Approved Solution	Approved By

Step Six: Integrate the PIA outcomes back into the project plan Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?		
Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns: