NHS
Rotherham
Clinical Commissioning Group

Title:	Information Security Policy
Ref No.	IT/007
Owner	Deputy Chief Officer
Author	Senior IG Specialist – eMBED Health Consortium
First issued on:	January 2017
Latest issue date	January 2020
Operational date	January 2020
Review Date	December 2021
Consultation process	IG Group to AQuA
Ratified and approved by	AQuA December 2019 Governing Body January 2020
Distribution	All staff and GP members of the CCG.
Compliance	
Equality & Diversity Statement	In applying this policy, the Organisation will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

1. INTRODUCTION

1.1 This document defines the Information Security Policy for NHS Rotherham CCG.

1.2 Whilst complying with current legislation and best practice this policy reflects that the CCG utilises a combination of locally managed information assets in addition to ICT services provided by The Rotherham NHS Foundation Trust (TRFT).

1.3 The purpose of information/cyber security is to ensure business continuity, to minimise the impact of security related incidents and to ensure the integrity of the information and data held by NHS Rotherham CCG. Information security enables information to be processed and shared with appropriate safeguards in place. It ensures the protection of information and assets as well as identifying and acting on threats to that security.

1.4 Information security refers to both technical and physical information. It ranges from the security of networks, to the use of appropriate passwords by staff and storage of confidential information in secure environments. This policy identifies employees' responsibilities for the security of information and encompasses the following components

- **Confidentiality:** assuring that sensitive information or data is accessible to only authorised individuals, and is not disclosed to unauthorised individuals or the public.
- **Integrity:** safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.
- **Availability:** ensuring that information, systems, networks and applications, as well as paper records, are available when required to departments, groups or users that have a valid reason and authority to access them.

2. PURPOSE

2.1 Effective information security management is essential to NHS Rotherham CCG. The purpose of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned, used or held by NHS Rotherham CCG by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other IT/IG policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2.2 This policy applies to all business functions within the CCG and all third party services that provide a service on behalf of the CCG. The policy covers data, information systems, networks, physical environment and relevant personnel who support these functions. It relates to both manual and electronic information, whether transmitted across the NHS private network, personal email addresses, or telephone lines, sent by fax, spoken in conversations or printed as hard copy.

3. DEFINITIONS

- **Confidentiality** - is defined as the restriction of information and assets to authorised

individuals.

- **Integrity** - is defined as the maintenance of information systems and physical assets in their complete and proper form.
- **Availability** - is defined as the continuous or timely access to information, systems or physical assets by authorised individuals.
- **Encryption** - is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.
- **Information Asset** - is defined as either personal information, corporate information, computer software, hardware, system or process documentation.
- **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 Officer on the security and use of those assets.
- **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.
- **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. floppy discs, CDs/DVDs, USB flash memory sticks or pens, PDAs.
- **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.

4. ROLES AND RESPONSIBILITIES

4.1 Chief Executive/Accountable Officer

The Accountable Officer is responsible for the management of information risk and information governance and is required annually to sign a compliance statement for the Annual Governance Statement with the Annual Report.

4.2 Senior Information Risk Owner (SIRO)

The Deputy Chief Officer is the SIRO for NHS Rotherham CCG and is responsible for information risk within the CCG. The SIRO advises the Governing Body and Chief Officer on the effectiveness of information risk management across the CCG. The SIRO has overall responsibility for ensuring that this policy is implemented, monitored and revised.

4.3 Data Protection Officer (DPO)

As a public body NHS Rotherham CCG is required to appoint a Data Protection Officer by the General Data Protection Regulation (GDPR). The Information Governance Policy establishes this role. The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The DPO reports to the SIRO and directly to the Governing Body in relation to data protection matters.

4.4 Information Asset Owners (IAO)

Local information assets will be assigned to a specific Information Asset Owner who shall be responsible for the information security of that asset. IAOs will be responsible for determining access controls for the asset and ensuring that authorised users are appropriately trained and made aware of their responsibilities with respect to maintaining information security and reporting any threats to security. Within the CCG IAOs will normally be senior staff members within relevant business units.

IAOs will:

- undertake regular information security training
- undertake regular reviews of risks to confidentiality, integrity and availability of the information asset on at least an annual basis
- provide the SIRO with assurance that information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks

4.5 Information Governance Lead

The Head of Health Informatics is the Information Governance Lead for NHS Rotherham CCG and is responsible for managing and implementing the policy and related procedures on a day to day basis with support from the Senior Information Governance Specialist from eMBED Health Consortium.

The Information Governance Lead will:

- ensure that staff are aware of their responsibilities and accountability for information security and provide support to the SIRO, IAOs and other staff
- ensure that the Information Security policy is maintained, reviewed and updated
- ensure that regular risk assessments for local information assets are completed and will monitor any potential and actual information/cyber security incidents and breaches

4.6 Information Security Lead

The IG Assurance and Security Manager at The Rotherham NHS Foundation Trust (TRFT) is the CCG's Information Security Lead under the Service Level Agreement between TRFT and the CCG for ICT services. The Information Security Lead can provide expert advice to the SIRO, IAOs and other staff.

4.7 The Rotherham NHS Foundation Trust IT Department

The Rotherham NHS Foundation Trust (TRFT) currently provides the CCG with ICT services. This Information Security Policy operates in conjunction with TRFT Information Security Policies and Procedures. Below is a summary of the TRFT's responsibilities for which the TRFT operates its own policies (further information is contained in the service contract):

- The TRFT IT department is responsible for ensuring that network computer equipment will be housed in a controlled and secure environment and protected with a combination of technical and non-technical measures.
- The TRFT IT department is responsible for ensuring that network backup procedures are documented and undertaken and that business continuity and disaster recovery plans are produced for the network.
- The TRFT IT department will provide NHS Rotherham CCG with regular

assurance that the services supplied to the CCG comply fully with the Information Security related requirements of the Data Protection and Security Toolkit (implementing the National Data Guardian's Security Standards).

- TRFT will provide NHS Rotherham CCG with assurance that regular risk assessments are undertaken with respect to the services and network supplied to the CCG.

4.8 All Staff

All staff are responsible for information security and therefore must understand and comply with this policy.

Each member of staff:

- shall be responsible for the operational security of the information systems they use and should ensure that they understand what information they are using, how it should be protectively handled, stored and transferred
- should ensure they understand what procedures, standards and protocols exist for the sharing of information with others
- shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard
- should ensure that they understand their personal responsibility for raising any information security concerns with the Information Governance Lead and know how to report a suspected breach of information security within the CCG.

4.9 Contractors and Other Organisations

Before the CCG contracts with external organisations to access the CCGs information systems a due diligence process must be completed and approved by the SIRO. External organisations cannot access the CCG's information systems without having a contract in place and a statement of works. The contract and statement(s) of work shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies and have a properly planned process before the work commences.

5. ACCESS CONTROL

5.1 Authorised Access

5.1.1 It is the responsibility of the IAO of each system to maintain satisfactory procedures for user access to that system. It is a general principle that users must always have individual access that is verified by a user name and password or alternative access controls such as Smartcards. In addition, the following must be observed, whenever relevant.

- All new starters to the organisation must receive a mandatory induction, which includes security and confidentiality awareness raising. It is the responsibility of all Line Managers to ensure that all new staff are properly inducted, and to arrange for access to all necessary information and communications technology (ICT) systems at an appropriate level, in line with relevant local procedures, to adequately perform their duties.
- Access to the computer account of other members of staff is only available in an emergency, and then only with verified authorisation from the Head of

Department/Service.

- All staff will have an email account. Access to the account of other members of staff is only available via proxy access with the permission of the user. Emergency access is only available with verified authorisation from Head of Department/Service.
- Email services should be used in accordance with the Email Usage Policy and Procedure.
- Access to the Internet and email services must be authorised by the Line Manager and accessed in compliance with the Internet Acceptable Use Policy.
- It is the responsibility of Line Managers to inform the TRFT IT Service Desk of any staff terminating their employment, immediately on notice being given to enable arrangements for removal of access.

5.1.2 It is good practice for the Line Manager to consult with the Information Governance Lead when deciding on the level of access that staff require, taking into consideration such issues as segregation of duties and sharing of expertise. Systems should have a clear role based access model to record which staff group have access to which parts of a system.

5.1.3 Where there is a requirement for an individual to have temporary access to any of the CCG's IT systems, (for example auditors and agency staff) the standard process for starters and leavers will be followed. Therefore the responsible staff member will be required to complete a network account request form prior to the start date and upon termination and forward this to the Office Manager for submission to the IT department.

5.2 Unauthorised Access

- Unauthorised access must be avoided at all times. To avoid unnecessary access, all users must either log out of all person based systems whenever not in use or left unattended or activate their password protected screensavers. Whenever screens are left unattended, users can also lock their screens by pressing Ctrl+Alt+Delete then Enter.
- Passwords must not be shared with other members of staff and must not be written down and/or left on display or be easily accessible.
- Smartcards must not be shared, and PIN numbers must be kept securely.
- If someone suspects that their ID and/or password security has been compromised they should immediately change their password and inform the TRFT IT Service Desk and/or the Information Governance Lead.
- Passwords must be changed regularly by users. Obvious choices of passwords or common words must not be used e.g. partner's, children's or pet's names etc.
- Passwords should be at least eight characters long and contain at least one numerical and one alphabetical character (Alphanumeric). They should never be written down or stored in an unencrypted electronic format. They should be changed at regular intervals with a maximum space of three months between changes.
- All passwords on any system should expire on a routine basis and users should be requested to change them. Where systems are not capable of doing

this the risk should be noted and mitigating controls identified by the system owner.

5.3 Computer Misuse Act 1990

Under the Act 'hacking' and the introduction of computer viruses are criminal offences. The purpose of the Act is to make provision for securing computer material against unauthorised access or modification. It makes unauthorised access to a computer, programs or data an offence. Staff should report any viruses, suspected viruses or suspicious emails (which could contain viruses) to the TRFT IT Service Desk. *(See appendix D for further guidance).*

6. INFORMATION SECURITY FRAMEWORK

6.1 Electronic Data Security

6.1.1 All contracts must include a confidentiality clause, binding staff to maintain a proper level of security to all sensitive and confidential information that they may encounter as part of their employment.

6.1.2 All data entered onto a system or captured manually must be held accurately and should conform to Data Quality guidance.

6.1.3 No data must be held that breaches the Data Protection Act 2018 (as enabled by the General Data Protection Regulation (GDPR)) or formal notification and guidance issued by NHS England. All personal identifiable information must also be used in accordance with the Caldicott Principles.

6.1.4 No member of staff will be allowed to access information until Line Managers are satisfied that they understand and agree the responsibilities under Data Protection legislation and organisational policies.

6.1.5 The CCG has a responsibility to ensure that data is held securely as a precaution against technical problems. Any files containing person identifiable information should be saved onto a network file server and not on the computer's local drive (i.e. C: Drive). This ensures that information is backed up on a daily basis. If staff do not have access to a network drive, it is the responsibility of the department or service to ensure information is backed up on a daily basis and this back up copy is encrypted and held securely. This should in these circumstances, contact the TRFT IT Service Desk or the Information Governance Lead for advice and guidance.

6.1.6 Staff should not store person identifiable information on mobile devices (e.g. laptops, PDAs, memory sticks etc). If there is a specific business requirement for this process, this should be documented as an information asset on the information asset register and be approved by the SIRO or Caldicott Guardian if the data is patient related. As a minimum the device must be installed with appropriate encryption software (requested through the TRFT IT Service Desk).

6.1.7 If there is a requirement to copy or transfer information between systems (whether bulk data or individual records) consideration should be whether this data transfer process triggers a requirement to conduct a Data Protection Impact Assessment which will take into account legal and technical requirements based on the risks and sensitivity of the information. This should be approved by the DPO and SIRO (include Caldicott Guardian if patient data is to be processed and reported to the Information Governance Group. As a minimum staff should ensure that any confidential information remains secure when in a static or during the transfer process and that the recipient system has the same or greater standard of security protection. Staff should also refer to the Internet Acceptable Use Policy and the Usage of Email Policy and

Procedure.

6.1.8 The TRFT IT Department will ensure all network drives on critical network servers will be backed up in accordance to written backup procedures and these will be stored securely.

6.1.9 Information that is no longer required should be disposed of or archived securely and in line with the Records Management Code of Practice for Health and Social Care 2016. Anything that contains personal and/or confidential information that does not require archiving must comply with local confidential waste procedures (i.e. shredding, use of confidential waste bins).

Staff should refer to the CCG's Confidentiality Code of Conduct and Data Protection Policy

6.2 Physical Security

6.2.1 All staff must wear identification badges at all times. Persons entering non- public areas should be challenged and asked to produce some form of identity or asked to sign into the building if on a specific business activity. Particular attention must be given to "tailgating" this is where an individual gains access to secure areas by closely following an authorised individual through a secured access point.

6.2.2 All computer assets including hardware and software must be recorded with the TRFT IT Service Desk.

6.2.3 Computer equipment must be sited appropriately to minimise the risk of damage such as fire, flood or accidental damage. Common hazards include drinks, food and overstraining of leads when a machine is moved.

6.2.4 Paper records must be filed in fire retardant filing systems.

6.2.5 Personal confidential information must not be left on desks when unoccupied. All confidential information must be locked away when not in use.

6.2.6 Staff who process personal confidential information on laptops and display units should be aware if the information is viewable to those who should not be reading it. When moving away from your computer you should ensure your screen is locked (see Appendix A) including when evacuating the building in an emergency.

6.2.7 All personal confidential information when printed, faxed or photocopied must be cleared from printers, faxes and photocopiers immediately and, when no longer required, destroyed securely in accordance with confidential waste disposal procedures.

6.2.8 When vacating meeting rooms or shared areas the area must be checked by the meeting participants to ensure that no data, regardless of format has been left behind. All whiteboards must be cleaned of information and used flipchart pages must be removed and disposed of securely.

6.2.9 On discovering any damaged or tampered with physical security devices, lost access fobs or ID badges, inform the office manager with immediate effect and complete an Incident Form.

6.3 Home, Mobile and Remote Working

6.3.1 As mobile devices are used off site, they are especially vulnerable to breaches of security. For this reason the additional points below must be followed:

- Users taking computer equipment off-site must follow the CCG's guidelines and in particular, equipment should not be left visible in unattended public places.
- Software installed on portable computers must be licensed to run the relevant packages.
- All mobile devices must have CCG approved encryption software installed and this can be requested via the TRFT IT Service Desk.
- Organisational approved anti-virus software must be installed and updated regularly and any external storage devices such as CD ROMs, floppy disks, USB Pens, memory sticks etc. must be checked for viruses on a regular basis.
- All users must take responsibility for backing up files held on portable computers on a regular basis.
- Portable devices should be 'docked' regularly; this will ensure that the device receives updates and that anti-virus software and encryption software is up to date.
- Use passwords on all systems and documents to minimise potential data exposure.
- Perform regular 'housekeeping' tasks such as backups, archiving and deleting old unneeded files (in line with retention and destruction schedules).
- Where ever possible keep your portable device out of sight to minimise the risk of theft. Never leave your portable device unattended especially in an unattended car or even in a locked boot, keep it with you at all times.
- Only authorised and licensed software and files may be installed and stored, this includes image files, screen savers and MP3 files.
- Mobile devices provided by the CCG should only be used for the purpose it was provided for and not used for non-work related tasks.
- Staff are responsible for mobile devices and any data held on it. In the unlikely event of loss or theft, inform Line Management with immediate effect and complete an Incident Form.
- Where mobile IT equipment is used in a public space, such as train or hotel, extra care must be taken to ensure the information on display cannot be overlooked or read by those around.
- If discussing CCG work off site, staff should be aware of who is around you and may overhear the conversation. Confidential information must not be discussed in public places where it might be overheard.
- Hard copy confidential information must never be left unattended, even at home, and must be locked away when not in use.

6.4 Disposal of IT Equipment, Media and Confidential paper

6.4.1 The disposal of IT equipment and devices should only be carried out through the IT department. Certificates of destruction should be supplied to the CCG to evidence the disposal of the device.

6.4.2 All data storage devices must be purged of sensitive data prior to disposal. Where this is not possible, the equipment or media must be returned to the TRFT IT for confidential disposal.

6.4.3 For confidential paper files which require disposal a number of confidential waste bins are situated throughout the premises for use.

6.4.4 TRFT and Confidential waste contractors are audited to ensure appropriate destruction processes are followed.

6.5 Virus Control

6.5.1 All organisations view viruses and other malicious software as presenting a significant threat to any system, and it is a disciplinary offence to willfully introduce a virus or other malicious software onto the organisation's computer systems.

6.5.2 Any external software brought onto the site must be virus checked using the approved anti-virus software. Where a virus scanner is available on the workstations users have the responsibility for checking external storage devices and any downloads. All organisational PCs are installed with virus checking software which is programmed to run daily.

6.5.3 E-mails are of particular concern as viruses from these are transmitted using attachments. Users must be vigilant when receiving unknown e-mails. Staff should refer to the CCG's Email Usage Policy and Procedures.

6.5.4 Users shall not install software on the CCG's property without permission from TRFT IT department or Information Governance Lead. Users breaching this requirement may be subject to disciplinary action. *See Appendix D for further details*

6.6 Monitoring System Access and Use

6.6.1 An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. NHS Rotherham CCG will put in place routines to regularly audit compliance with this and other policies. In addition it reserves its right to monitor activity where it suspects that there has been a breach of policy.

6.7 Business Continuity

<u>Business Continuity Plans</u>

6.7.1 Business Impact Analysis will be undertaken in all departments of NHS Rotherham CCG. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

6.7.2 The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

<u>Back-up procedure</u>

6.7.3 All designated sensitive and critical systems must have written back-up procedures and a disaster recovery plan. This is required to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

6.7.4 All systems must be backed-up at regular intervals. Backups must be stored in approved locations and restore of back-ups should be tested regularly. All system require documented Recovery Time Objectives (RTO – the targeted duration of time which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity) and

Recovery Point Objective (RPO – the maximum targeted period in which data might be lost from an IT service due to a major incident).

7. INFORMATION, TRANSITION AND NETWORKS

7.1 Local and Wide Area Networks

7.1.1 Through connection to the CCG's network it is possible to receive and forward information to other users of the network and other organisations' networks using, for example, electronic mail. Should employees receive, identify how to, or gain access to unauthorised information on any networks then this event must be reported to the TRFT IT Service Desk.

7.1.2 All computer files transferred from other networks must be checked for viruses before use within the CCG.

7.1.3 All employees must inform the TRFT IT Service Desk if a virus is detected or suspected.

7.2 Internet and Email

7.2.1 The internet is a powerful tool, and the CCG is committed to supporting users with genuine business needs to gain access to the internet. However, it must be recognised that there are very real dangers in granting unrestricted access to the Internet for a variety of reasons.

7.2.2 The e-mail system enables employees to benefit from efficient office communication and should not be abused. Care should be taken when using electronic mail as e-mail is identical to, and has the same status as any other form of the CCG's business correspondence.

Refer to Policy on the Acceptable Use of the Internet and Email Usage Policy and Procedure for further guidance.

8. INFORMATION ASSET MANAGEMENT AND RISK ASSESSMENT

8.1 NHS Rotherham CCG will compile and regularly review an Information Asset Register covering information assets holding sensitive or personal data.

8.2 All local information assets will be identified and assigned an Information Asset Owner (IAO). IAOs shall ensure that information risk assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). This should be increased to quarterly for any 'High Risk' assets. IAOS shall submit the risk assessment results and associated mitigation plans to the SIRO for review.

9. ACCREDITATION OF INFORMATION SYSTEMS

9.1 The CCG shall ensure that all new information systems, applications and networks include a Privacy Impact Assessment (PIA) and System Level Security Policy (SLSP) and are approved by the Information Governance Group and/or TRFT IT before they commence operation.

9.2 When planning for, and during procurement of, new systems, it is the responsibility of the Project Manager or Lead to ensure that appropriate system security features are

included within the system. As a minimum this will include a password protection feature and audit logs.

9.3 Systems and applications must be adequate for their purpose.

9.4 Software applications, upgrades and amendments must be developed in a controlled manner, documented and thoroughly tested before implementation.

9.5 Proof of ownership of software licenses must be maintained and master disks held by TRFT in a secure environment in the event of necessary re-install.

9.6 Unauthorised software must not be introduced onto any system without prior authorisation from the TRFT IT Service Desk.

10. TRAINING

10.1 Data Security Awareness training is mandatory and all staff are required to complete annual online Data Security Awareness training.

10.2 Additional specialist training will be undertaken for staff with specific Information Security roles and responsibilities; including Information Asset Owners, SIRO and Information Governance Lead.

11. RELEVANT LEGISLATION

11.1 This policy is designed to support NHS Rotherham CCG's compliance with the following legislation:

- The Data Protection Act (2018) (as enabled by the General Data Protection Regulation (GDPR)
- The Computer Misuse Act (1990)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health and Social Care Act 2012
- Health and Social Care Act (Safety and Quality) 2015
- Records Management Code of Practice for Health and Social Care 2016

12. RELATED POLICIES AND PROCEDURES

- Confidentiality Code of Conduct
- Data Protection Impact Assessment procedure
- Policy on the Acceptable Use of the Internet
- Email Usage Policy and Procedure
- Incident Reporting Policy
- Portable Device, Smartphone and Tablet Policy

13. MONITORING

13.1 It is the responsibility of all staff to ensure that the potential for security breaches does not occur as a result of their actions. All staff must report instances of security breaches, near misses or weaknesses through the incident reporting procedures.

13.2 The Information Governance Group will report information security incidents to the SIRO and Caldicott Guardian.

13.3 Information Governance and TRFT IT will investigate all suspected/actual security breaches and report to the appropriate bodies.

13.4 The CCG will be responsible for collating and reporting the number of breaches and ensuring actions have been taken.

13.5 TRFT IT will in conjunction with departments provide advice and guidance on how to maintain security and confidentiality compliance across organisations. Where technical staff are asked to install software onto machines connected to the network, proof of purchase and licensing will be required.

Refer to the organisation's Incident Reporting Policy for further details.

14. REVIEW

14.1 This policy will be reviewed every two years. Any amendments to the policy will be recommended by the Information Governance Group. The policy will be approved by the Audit and Quality Assurance Committee and ratified by the Governing Body.

APPENDIX A – Good Practice Guide for Staff

This section is intended to be an aide to employees by listing some of the common aspects of the security policy. It is not intended to be a comprehensive summary and does not reduce or alter the standards or principles laid out in the Information Security Policy.

- Contact your Line Manager if you are aware that you are not meeting the standards and principles of the security policy.
- All staff must attend mandatory training sessions that are made available to them and identify areas of training need regarding information and security issues.
- Be aware of potential risks that surround the data and systems that you use – remember it is your responsibility to keep personal data confidential.
- Where possible, store all data to the network file servers and not on personal computer 'C' drives as these drives are backed up on a daily basis. If you do not have access to a network file server, please contact the TRFT IT Service Desk and/or the Information Governance Lead.
- Safeguard portable IT equipment, memory sticks and external storage devices. Do not leave them visible in unprotected areas. These devices must be encrypted.
- Dispose of confidential information on printouts, external storage devices in a secure manner and in line with confidential waste procedures.
- Always log off or lock by pressing the Microsoft Windows Flag key (⊞) + L if you leave your computer unattended. The Microsoft Windows Flag key is located on the lower level keys of a standard keyboard.
- Passwords must be kept secure at all times and **never** written down or shared with anyone else.
- Wear your identification badge at all times and challenge strangers without one.
- Observe building security procedures. Close and lock windows and doors when unattended and ensure curtains and blinds are drawn, if applicable at night.
- All files that are either downloaded or sent in e-mail attachments must be virus checked along with any external device prior to opening on the PC.
- Do not hold personal information on your computer system without approval from the Caldicott Guardian and an understanding of the principles of the Data Protection Act and GDPR, and confirming that there is sufficient physical security in place.

APPENDIX B – Guidelines to the Six principles under the Data protection Act 2018 and General Data Protection Regulation from 25th May 2018)

First Principle - Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals	a) Ensure that information is only used for the purpose it was intended. b) Provide all persons with information on their rights as data subjects – why you are collecting their data and what you intend to do with it and who you intend sharing it with.
Second Principle – Personal data can only be collected for specified, explicit, and legitimate purposes. This data can only be used for those described purposes	a) Ensure that people are aware why you ask them for their information.
Third Principle – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	a) Wherever possible we should only record the minimum amount of information that is required in order to fulfil the purpose.
Fourth Principle – Personal data shall be accurate and, where necessary, kept up to date.	a) It is our responsibility to ensure that data held about individuals is accurate, and not misleading. b) Where appropriate information should be
Fifth Principle - Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.	a) Review what data is held regularly and delete the information which is no longer required. b) Be aware however, certain types of information have specified retention periods.
Sixth Principle – Appropriate technical and organisational measures shall be taken against unauthorised or lawful processing of personal data and against accident loss or destruction of, or damage to, personal data	a) All measures must be taken to ensure a level of data security appropriate to the nature of data to be protected. Consideration must be given to the potential harm that may result in a breach of security.

APPENDIX C – Caldicott Principles

The Caldicott report was published in 1997 on Protecting and Using Patient Information and has been adopted by the NHS as HSC 1999/012.

One of the key requirements of the recommendations was the appointment of a Caldicott Guardian in every NHS organisation. The Caldicott Guardian is responsible for implementing and monitoring achievement of the recommendations laid down in this report. The main recommendations fall mainly into 3 categories.

1. Training and awareness of Security & Confidentiality along with induction of new staff and inclusion of compliance within the contract of employment. Information published to patients/clients informing of the proposed use of information.
2. Review and justify use all information flows including external organisations ensuring correct protocols in place for sharing information
3. Access control, security monitoring, incident reporting procedures and risk management, including user responsibilities

A set of principles was developed, against which every flow of patient-identifiable information should be regularly justified and tested. A further review of the use of information in the NHS was undertaken by Dame Fiona Caldicott in 2013; following which a seventh principle was added.

Principle One – Justify the Purpose.	Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
Principle Two – Don't use patient-identifiable information unless it is absolutely necessary.	Patient-identifiable information items should not be used unless there is no alternative.
Principle Three – Use the minimum necessary patient-identifiable information.	Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing the risk of an individual being identified.
Principle Four – Access to patient-identifiable information should be on a strict need to know basis.	Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see in order to carry out their job role.
Principle Five – Everyone should be aware of their responsibilities.	Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are aware of their responsibilities and obligations to respect confidentiality at all times.
Principle 6 - Understand and comply with the law.	Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.
Principle 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 D – Good Practice Guidelines for Dealing with Viruses

1. What is a computer virus?

Computer viruses are called viruses because they share some of the traits of biological viruses. They pass infection from computer to computer like a biological virus passes from person to person. A computer virus must piggyback on top of some other program or document in order to get executed. Once it is running, it is then able to infect other programs or documents.

2. How does it spread?

Such documents or programs can be transferred in many different ways, including the following:

- Via an email attachment
- Via items downloaded from the Internet
- Via an external media source, i.e. a floppy disk or compact disk

3. What should you do if you have or suspect a virus?

DO

- Call the TRFT IT Service Desk immediately if you find or suspect a virus.
- If out of hours switch your PC off if you find or suspect a virus, unless use of your computer is essential, and contact the Service Desk as soon as possible thereafter.
- Ensure that, except under exceptional circumstances, only devices officially purchased by your organisation are inserted into the drives of the organisation's computers.
- Ensure that other devices, including any disk or data stick that has been inserted into the drive of any non-organisational computer, should never be used without good reason.
- Virus check any devices that have not been officially purchased by your organisation and/or have been inserted into the disk drive of a non-organisational computer.
- If necessary take disks or data sticks to the TRFT IT team to be scanned.
- Try to limit the number of devices you pass around internally or externally. It helps if the number of suspect virus carrying devices are traceable. Only use these types of device to transfer files between computers if you really have to.
- Ensure your data is stored on the network drive so that should the worst happen and your computer is infected by a virus your files can be retrieved from backup copies.

DON'T

- Don't panic. If you do find or suspect a computer virus then it can generally be removed.
- Don't use any device in an organisations computer that hasn't been officially purchased by that organisation without first having it checked for viruses.
- Don't load any non-organisational authorised software onto any computer. This means non-organisational approved applications, PC Games or Screensavers, whether they are from a mobile device, via an email attachment or downloaded from the web. If you are unsure whether the software you wish to load is authorised, call the TRFT IT Service Desk.
- Don't leave a compact disk in the drive when you switch off your computer.
- Don't try to remove the virus yourself by use of your own, or someone else's anti-virus software. You could make matters worse.

- Don’t open an e-mail attachment unless certain of its source and content.
- Don’t connect your laptop computer to another organisations network without approval from TRFT IT Service Desk.

4. User procedures for reporting a suspected virus.

- If you suspect a computer virus:
- Contact the IT Service Desk immediately
- If out of hours, unless use of the PC is essential switch your machine off and contact the Service Desk as soon as they become available.
- Do not send or forward any further mail.
- Make a note of any messages or events which have caused you to believe that your PC contains a virus.
- If you suspect the virus has been transferred as an email attachment, make a note of the senders address and if appropriate who else the email has been distributed to.
- Do not use the email system until instructed it is safe to do so by a member of the TRFT IT Service Desk.

APPENDIX E – Equality Impact Assessment

Title of policy or service:	Information Security Policy	
Name and role of officer/s completing the assessment:	Andrew Clayton – Head of Digital	
Date of assessment:	20/12/2019	
Type of EIA completed:	Initial EIA 'Screening' ☒ *or* 'Full' EIA process ☐	*(select one option - see page 4 for guidance)*

1. Outline	
Give a brief summary of your policy or service Aims Objectives Links to other policies, including partners, national or regional	Effective information security management is essential to NHS Rotherham CCG. The objectives of the Information Security policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned, used or held by NHS Rotherham CCG

Identifying impact:
Positive Impact: will actively promote or improve equality of opportunity;
Neutral Impact: where there are no notable consequences for any group;
Negative Impact: negative or adverse impact causes disadvantage or exclusion. If such an impact is identified, the EIA should ensure, that as far as possible, it is either justified, eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.					
(Please complete each area)	What key impact have you identified?			For impact identified (either positive and or negative) give details below:	
	Positive Impact	Neutral impact	Negative impact	How does this impact and what action, if any, do you need to take to address these issues?	What difference will this make?
Human rights	☐	☒	☐	N/A	
Age	☐	☒	☐	N/A	
Carers	☐	☒	☐	N/A	
Disability	☐	☒	☐	N/A	
Sex	☐	☒	☐	N/A	
Race	☐	☒	☐	N/A	
Religion or belief	☐	☒	☐	N/A	
Sexual orientation	☐	☒	☐	N/A	
Gender reassignment	☐	☒	☐	N/A	
Pregnancy and maternity	☐	☒	☐	N/A	
Marriage and civil partnership (only eliminating discrimination)	☐	☒	☐	N/A	
Other relevant groups	☐	☒	☐	N/A	
HR Policies only: Part or Fixed term staff	☐	☒	☐	N/A	

IMPORTANT NOTE: If any of the above results in 'negative' impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues/impact identified	Actions required	How will you measure impact/progress	Timescale	Officer responsible

4. Monitoring, Review and Publication				
When will the proposal be reviewed and by whom?	Lead / Reviewing Officer:	Andrew Clayton	Date of next Review:	December 2021

Once completed, this form must be emailed to Alison Hague, Corporate Services Manager for sign off: Alisonhague@nhs.net

Alison Hague signature:	