Northamptonshire Healthcare NHS
NHS Foundation Trust

Use of Information and Communications Technology Policy

Table of Contents

Why we need this Framework

Northamptonshire Healthcare NHS Foundation Trust (NHFT) has a legal obligation to comply with all appropriate legislation in respect of data protection, information governance and information Security. It also has a duty to comply with guidance issued by the Department of Health, the Information Commissioner, other advisory groups to the NHS and guidance issued by professional bodies.

What the Framework is trying to do

The purpose of this policy is to provide a single overarching use of information and communications technology policy. This policy applies to staff, patients, visitors, students and volunteers that access information and information technology.

Maintaining confidentiality and preserving information security is essential to the Trust being able to supply an exceptional confidential service that delivers the highest quality patient care.

Which stakeholders have been involved in the creation of this Framework

- Information Governance Planning Group
- IM&T Programme Board

Any required definitions/explanations

- Computer Misuse Act 1990 (amended in 2005)
- Copyright, Designs and Patents Act 1988
- Children' Act 2004 and the Children and Young Person Act 2008
- NHS Trusts and PCT's (Sexually Transmitted Diseases Regulations) 2000
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Re-Use of Public Sector Information Regulations
- Records Management Code of Practice for Health & Social Care 2016
- Confidentiality NHS Code of Practice 2003
- Information Security Management NHS Code of Practice

Data Protection Legislation Definitions
Data Protection Legislation includes (i) The Data Protection Act 1998 up to and including 24 May 2018, and (ii) the General Data Protection Regulations (GDPR) from 25 May 2018 (iii) The Data Protection Act 2018 when it comes into force and any secondary legislation as amended or updated from time to time (iv) any successor legislation to the GDPR or the Data Protection Act 2018.

Malicious Software
Malicious software is defined as any software or piece of programming that is intended to be disruptive or destructive to a single computer or any part of organizations Technical Infrastructure.

NHFT
Northamptonshire Healthcare NHS Foundation Trust.

Personally Identifiable Data (PID)
Is information that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance Number and photographs.

Safe Haven
The term safe haven is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely

Special Category Personal Data (Sensitive Personal Data)
The General Data Protection Regulations (GDPR) refers to sensitive personal data as "special categories of personal data". The categories defined are, namely, personal data consisting of information as to:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Trade union membership
- Genetics (where used for ID purposes, excl. personal data relating to criminal convictions and offences)
- Biometrics (where used for ID purposes, excl. personal data relating to criminal convictions and offences)
- Physical or Mental Health
- Sexual life or sexual orientation

Social Media
Term used to describe the use of mobile and web technologies to communicate and share information.

Trust
The word Trust relates to Northamptonshire Healthcare NHS Foundation Trust.

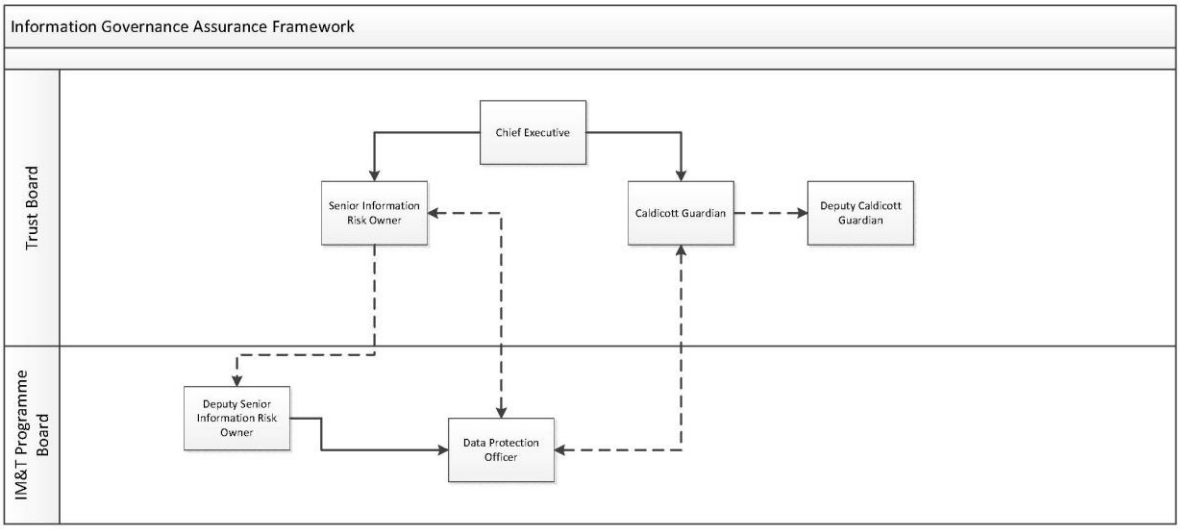
Virus
A virus is a malicious program that has the ability to reproduce itself and infect other programs or storage devices. Typically a virus will not show itself immediately, but will add itself to programs and disks to spread widely on many computers before it is triggered into its destructive phase.

VPN
Virtual Private Network is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wire.

Key Duties

The Chief Executive

The Chief Executive has the ultimate responsibility of the management of the Trust and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The Trust has a specific responsibility for ensuring that it corporately meets its legal responsibilities, and for the implementation of internal and external governance requirements.



Senior Information Risk Owner (SIRO)

The SIRO will act as an advocate for information risk on the Board and in internal discussions will lead on the annual programme of work to asses and work to minimise information risk.

Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Chief Information Officer

The Chief information officer (CIO) role has the responsibility for developing information technology (IT) strategy and maintaining the computer systems required to support an enterprise's objectives and goals.

Head of Clinical Systems & Governance

The Head of Clinical Systems and Governance is responsible for advising on the strategic direction in relation to information security and governance, the development of policy and guidance and providing operational support to the Trust.

Responsibilities also include maintaining the Trust's Information Assets Register, ensuring that it remains up to date and supporting the SIRO in ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist. This role also encompasses responsibility for acting as the Data Protection Officer for the Trust as directed by the General Data Protection Regulation.

Department Heads, Service and Line Manager

It is the responsibility of Department Heads, Service and Line Managers to ensure that the contents of this policy and its accompanying procedures are discussed e.g. at staff forums, and possible implications for service delivery are identified and acted upon

Responsibilities also include ensuring that all copies of personal information are accurate and kept up to date. Also that information is securely handled including obtaining, recording, storing, retrieval, consultation, holding, disclosing, use, transmission, erasure, destruction.

Information Asset Owners

Information Asset Owners have been identified by their level in the organisation and their role in protecting the Trust Information Assets. Information Asset Owners have responsibility to ensure that policies and procedures are followed, recognise actual or potential security incidents and threats, and ensure that information asset registers are accurate and up to date.

Each Information Asset Owner can assign day to day responsibility for each information asset to an administrator or manager.

All Staff, Students, Volunteers and Third Parties

All employees and anyone working on behalf of the Trust, involved in the receipt, handling or communication of person identifiable information and commercial information, has a duty to adhere to this policy. Personal responsibility to act in accordance with the Data Protection Act http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted must be considered at all times. Everyone has a responsibility to escalate to their line management where a process defined in this policy is not being adhered to.

Responsibilities also include ensuring that all copies of personal information are accurate and kept up to date. Also that information is securely handled including obtaining, recording, storing, retrieval, consultation, holding, disclosing, use, transmission, erasure, destruction.4

All Patients and Visitors

Maintaining proper records is vital to patient care. If records are inaccurate this can result in delays in your treatment. It is important that you provide us with complete and accurate information, and let us know if your circumstances change**.**

Framework detail

Confidentiality, Data Protection and Sharing Information

We are required to keep some information about patients, which we use to help us to provide care and to help us monitor the way we run our services. While we are providing care, the referrer will be kept informed of each patient's progress unless specifically asked not to. We may also need to share information with other agencies, such as social services, which may provide care.

If a patient is deemed capable of giving consent to treatment we will provide as much information as possible and get their agreement before performing any procedure. If patients are deemed capable of refusing treatment we will respect these wishes.

For patients who are unable to give consent, we do our best to consult a next of kin or an advocate about any serious treatment we need to give. Parental consent will usually be sought for children requiring treatment. In certain circumstances, however, such as in an emergency, treatment will be provided without consent if we think it is in the patient's best interests.

Gillick competency and Fraser guidelines can be used to support decisions of capacity for children. Additional guidance on this can be found in the below **Consent to Examination or Treatment information** guidelines:

https://www.gov.uk/government/publications/reference-guide-to-consent-for-examination-or-treatment-second-edition

Confidentiality

There are four basic rules for making a lawful disclosure of confidential Information:

- Where an individual to whom the information relates has consented.
- Where the disclosure is in the public interest
- Where the disclosure is in the best interest of a service user who lacks the capacity to provide consent
- Where there is a legal duty to do so (court order)

There are exemptions under the Data Protection Legislation where disclosure without consent is allowed, but must be balanced against responsibilities under the Common Law Duty of Confidentiality

The Caldicott Guardian and the Head of Clinical Systems and Governance should be approached for advice relating to the use and disclosure of confidential information where there is a concern whether information should be shared.

When processing patient identifiable information, all NHFT employees and volunteers are required to follow the 7 Caldicott Principles:

- Principle 1 – Justify the purpose for using confidential information
- Principle 2 – Only use it when absolutely necessary
- Principle 3 –Use the minimum that is required
- Principle 4 – Access should be on a strict need to know basis
- Principle 5 – Everyone with access to patient identifiable information should be aware of their responsibilities
- Principle 6 – Understand and comply with the law
- Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality

Data Protection

The Data Protection Legislation sets out the terms and conditions under which personal identifiable data relating to a living individual will be handled, or processed. The Act applies to the collection, use, disclosure, retention, storage and destruction of data and created 6 principles to make the legislation clearer for organisations and individuals to follow. All staff and volunteers must follow the eight data protection principles outlined below:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Further information on the **6 Data Protection Principles** can be found on the Information Commissioner's Office website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Sharing Information

The Trust will develop Information sharing agreements to support the safe sharing of personal information between organisations. Information sharing agreements set out a common set of rules to be adopted by the various organisations and require each organisation to sign that they agree.

Before entering into any information sharing arrangement, the Trust will complete a Data Protection Impact Assessment (DPIA). This will help to assess the benefits and any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

All Information Sharing Agreements will be added to the Trusts Information Sharing register maintained by the Information Governance Team.

The absence of an Information Sharing Agreement should not prevent the sharing of information where a legal basis exists. If in doubt please contact the Information Governance Team.

Record Retention

The Trust is required to keep information in accordance with the timescales set out in the Records Management Code of Practice for Health and Social Care.

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Documents that contain personal data that are not listed within the Code of Practice need to have a retention period set by the organisation for advice and guidance contact the Information Governance Team.

Subject Access Requests

The Trust recognises the individual's right of access to health information and in some cases to health information relating to other people. The Trust will ensure that support is given to service users to exercise this right. The Data Protection Legislation gives the individuals or their authorised representatives the right to apply to view or have copies of personal data held about them, including health records.

The Trust recognises that information relating to the deceased, where there is a legitimate interest is accessible through the Access to Health Records Act 1990.

The Trust will accept written requests, including e-mail, from a patient for access to their information. The Trust will make a standard access form available to the public to assist application. Telephone requests from an individual who is unable to make a written request will be accepted subject to strict conditions following the Department of Health Guidance for Access to Health Records 2010. The Trust may require applicants to provide proof to establish their identity.

Where an application is made on behalf of a patient the Trust will confirm that the consent of the individual had been obtained prior to any release. When an individual has not specified the information that they require the Trust reserves the right to ask the applicant to refine the request.

All employees are responsible for compliance with statutory timeframes under the terms of the Data Protection Legislation.

Where an access request has previously been met and a subsequent identical or similar request is received the Trust will assess if a reasonable time interval has elapsed before providing the information.

For more information on how to make an application for access to personal information that the Trust holds:

https://www.nhft.nhs.uk/foi

The Trust may extend the time period for providing a response to a Subject Access Request by up to 2 months where a request is considered to be complex or where the data subject has made a number of requests. The Trust will inform the data subject within one month of receiving a request if this is the case and explain why the extension is necessary. Whether a request is complex will be considered on a case by case basis.

Freedom of Information

The Freedom of Information Act (FOIA) became law on 1 January 2000 and came fully into effect on 1 January 2005. The FOIA provides a general right of access to all non-personal information held by public authorities. The Trusts Publication scheme and details of how to make a FOIA request are available at:

https://www.nhft.nhs.uk/foi

The Act includes exemptions to the general right of access. These exemptions can be used by the Trust when requests are made for information which is considered to be commercially sensitive or where the resources to complete a response exceed the national limit of 18 hours.

Further information on the exemptions to the act can be found on the Information Commissioner's Office website:

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a- request/

Corporate Records Management

Corporate records management refers to the process and standards by which an organisation handles its corporate records. For NHFT a corporate record can be considered as, any information that is recorded by staff members within the Trust as part of their work, this can be in any media format, for example:

- Financial/Accounting records
- Emails
- Computer databases, output portable storage media and all other electronic record
- Material intended for short term use including handwritten notes before they are added to a formal record.
- Photographs and other images

All staff members within NHFT must ensure that corporate records are handled in line with the principles of the Data Protection Legislation, as well as in compliance with the Freedom of Information Act and the NHS Records Management Code of Practice for Health & Social Care 2016.

Access and Authorisation

Every member of staff will have authorised access to IT systems based on work roles and needs. This process is initially identified through NHFT's Starters and Leavers forms and includes authorisation from the line manager.

Access to information is restricted only to those authorised to see it. Do not access or help anyone else to access any computer system or modify any programme or data unless you are authorised to do so. This is an offence under the Computer Misuse Act 1990 and could lead to prosecution.

It is strictly forbidden for employees to use NHFT systems to knowingly browse, search for or look at any personal or confidential information relating to themselves, their own family, friends or other persons, without a legitimate Trust purpose. Action of this kind will be viewed as a breach of confidentiality and will likely result in disciplinary action being taken.

Use of equipment and systems

All Trust staff and volunteers must ensure that they use only Trust approved and asset tagged IT equipment on the Trust network this includes but is not limited to Laptops, Mobile phones and Tablets. The asset number for a device will be generated from an asset tag or a number unique to the device.

In addition the only memory sticks permitted onto the network are the encrypted devices that are provided by the Trust which are encrypted to industry standard. All approved devices will be installed with encryption and virus and threat monitoring software.

All access to Trust network and devices is granted for business need this includes but is not limited to WIFI, and mobile data networks. Trust users are bound by the same rules of confidentiality and security whilst away from their place of work as when they are at their desk. To access the Trust network when away from Trust sites users will need to be set up through the IM&T ServiceDesk with Virtual Private Network (VPN) Access.

Workstation

If a computer or tablet device is left logged on it is easy for anyone to gain unauthorised access to data or change or delete files. Trust network users must not leave their workstation unattended without locking it by using the following method that works on both computers and laptops:

- Control Alt Delete – Lock Workstation

- Unlock Workstation – Control Alt Delete – Enter Password

Mobile Devices

Users must ensure their mobile device is stored and used safely and securely and that any personal data is protected. This includes setting a personal password. Staff should contact the IM&T Service Desk for assistance if needed.

Each user that is allocated a mobile phone or tablet device will be required to accept the Mobile Device Terms and Conditions these are included in Appendix A for further reference. Acceptance of the terms and conditions is a requirement of receiving a device. Each user has a responsibility to read these and ensure that they safeguard the device and information that it holds.

- Users must not lend or allow their device to be used by anyone, other than permitted work colleagues.
- Users must not attempt or allow any unauthorised repairs to Trust equipment.

Multiple devices per user will require authorisation at Deputy Director Level. Where it is identified that a user has a number of devices of the same type then a process will be followed to determine business need and seek approval as appropriate. Where a user requires a replacement device it will be expected that the original device is released to the deploying technician at the point the new device is issued or the user will sign to confirm that they will return the device to IM&T Business Services within 10 working days.

Managers have a responsibility to return all devices associated with a leaver to IM&T ServiceDesk this enables equipment to be assessed for reallocation or destruction. Further information is available on the Staffroom.

Lost, Stolen and Damaged Devices

You must not delay in reporting if a device is lost or stolen via logging a call with ServiceDesk and raising a Datix. This will enable information stored on the device to be remotely wiped and removed. Notification needs to take place within 24 hours of identifying a device is lost or stolen. A Datix incident will be raised.

Replacement devices for lost, stolen and damaged devices incur a cost to the Trust.

Internet Use

The Trust may limit or deny access to internet services for personal use, such as internet banking, personal webmail and social networking to maintain business use of the Internet or for any other reason at its absolute discretion. The Trust reserves the right to monitor and audit all use of the internet on its network.

There is a list of approved mobile phone apps that have been subject to a Data Protection Impact Assessment for APP's that store or share data is available on the Staffroom. Mobile devices must primarily be used for business purposes. For further advice please contact the IM&T ServiceDesk or Information Governance team.

Email Use

Emails form part of the written corporate record of the Trust and they may be released in part or whole

to a wider audience or used as evidence in legal proceedings. E-mail is capable of forming or varying a contract in just the same way as a written letter, this gives rise to the danger of employees inadvertently forming contracts on behalf of NHFT or varying contractual terms in which NHFT then becomes bound.

Every user of e-mail has the responsibility to ensure that they practice proper use of the e-mail system, and that they are responsible for:

- Any e-mails they create or amend.
- Understanding when e-mail is strictly prohibited.
- Recognising that any emails they create are not their personal property, but belong to NHFT, and maybe subject to public disclosure.
- Complying with good housekeeping routines to manage their mailboxes appropriately, ensuring that e-mails are actioned, deleted or permanently stored on the Network in shared drives for reference purposes.
- Taking due care and attention when sending, receiving, amending and storing all e-mail transactions.
- Not sending messages or attachments that could be deemed libellous, defamatory, harassing or pornographic
- Not sending information in breach of Copyright legislation
- Sending sensitive and confidential information securely in line with the Trust email procedure.
- Not sending inaccurate information about an individual or organisation.
- Not sending trust Corporate or sensitive information to personal email accounts

For further information on staff responsibilities see the Trust Email Procedure.

E-Safety

There is a requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely. The use of new technologies can put young people at risk. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

The Trust will include e-safety awareness into its Safeguarding training to raise awareness of staff. E-safety incidents identified by staff must be reported on Datix and investigated in line with Trust policy.

Guest Wi-Fi

NHFT provides guest Wi-Fi in various trust sites. Access to the network is granted with the following considerations.

- NHFT does not guarantee the security, confidentiality or the integrity of a user's information on the guest wireless network.

- NHFT is not responsible for the loss, misuse or theft of any information, passwords or other data transmitted by users through the guest wireless network.

- Access to the internet via the NHFT guest wireless network is monitored for inappropriate material and sites which are deemed to contain unsuitable material will be blocked.

- Access to the network will be blocked where it is suspected that an e-safety incident has taken place

Use of Social Media

The risk of social media is that once information is posted onto social media sites the information is in the public domain. Access to the information cannot be controlled by the Trust nor would the Trust have control over the archiving and retention of this information.

Where your comments or profile can identify you as a NHFT employee or volunteer you must make sure that you do:

- disclose your status during discussions relating to NHFT and its work
- This is to ensure that other users are aware of your back ground and reasons for interest in the topic.
- only disclose and discuss publicly available information.
- ensure that all content published is accurate and not misleading.
- be polite and respectful to all people you interact with.
- not disclose any confidential information.
- not post material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a court suppression order, or is otherwise unlawful.

Information Security

Effective information security involves more than simply installing a security product, implementing anti-malware software, providing a security policy or signing a contract with a support service provider. The Trust will assess its information Security as part of its IM&T work programme and will feed into the evidence provided for the annual Data Security & Protection Toolkit (DS&P) submission.

Improvements will be made as part of the annual review to Trust processes and physical IT measures to safeguard, all information assets, including patient records and other NHFT corporate information, from potentially harmful threats, whether internal or external, deliberate or accidental.

Virus Protection

The threat of damage to important business information and sensitive patient data from malicious computer viruses is increasing as the number of personal computer based applications grows. NHFT will protect its information systems from the introduction of computer and network viruses and other malicious software through the use of computer virus checking software and related procedures.

It is a requirement that PC's and laptops are connected regularly (at least once a month) to the network. This is to ensure that they will be automatically updated with the latest virus protection software and software patches. Laptops not connected regularly to the network must receive a health check before reconnection to the network. This needs to be pre-booked through the IM&T Service Desk.

System Backup

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, data entry errors, or system operations errors. Systems will be backed up in response to the information held and how regularly they are updated.

System Procurement

IM&T must approve all Trust purchases of nonstandard equipment and software. This is to ensure that the introduction of incompatible equipment which might affect the performance or functionality of existing systems does not occur. All security issues will be identified and considered during the requirements phase of a project during the completion of a Data Protection Impact Assessment (DPIA). The relevant issues will then be agreed and documented as part of the business case for the information system.

Information Asset Management

The management of information assets is crucial in achieving a secure information handling and management structure within the organisation. To ensure the Asset Register remains current, accurate and complete it will be subject to a rolling programme of review linked to the IG Toolkit submission. IAOs should undertake regular reviews to manage the information risks associated with their relevant assets.

Registration Authority/Smartcards

The Registration Authority (RA) is administered from within the Clinical Systems Team (CST) and the team is responsible for ensuring that all aspects of registration services and operations are performed in accordance with national policies and procedures, along with providing arrangements that will ensure tight control over the issue and maintenance of electronic Smartcards.

https://digital.nhs.uk/Registration-Authorities-and-Smartcards

Role	Responsible for	Name
Board/EMT Accountable	The Board/EMT individual must report to the Board/EMT annually on RA activity and must sign off on RA IG Toolkit submissions.	Richard Wheeler
RA Manager(s)	Running the governance of RA in the organisation, agree and sign off on local operational processes and should assure themselves regularly that these processes are being adhered to, registering RA staff in their own organisations and any RA Managers in child organisations, ensuring the effective training of RA Agents and Sponsors within their organisation.	Sarah Ratcliffe Lisa MacPhail

Caldicott Guardian	This is a smartcard specific role that enables the user to action Caldicott Guardian tasks on SystmOne. These tasks include assessing requests to delete clinical record entries. This is a delegated role on behalf of the NHFT Caldicott Guardian performed by CST and Information Governance.	Alex O'Neill-Kerr Sarah Ratcliffe Adam Shelley Lyn Bivens Danielle Mac

Smartcard Use

NHS Smartcards must be kept at all times with the user. Under no circumstances can Smartcards be:

- Issued without the organisation name
- Issued without the user's UUID and a true likeness of the user's photograph displayed and the users identity being proved in line with requirements set by NHS Employers
- Remain in the Smartcard reader when the workstation is unattended by the user
- Only the end user whose name is on the Smartcard should know their passcode for their Smartcard. If anyone else knows the end users passcode it breaches the Smartcard terms and conditions of use and the Computer Misuse Act 1990.

It is mandatory that all users sign the Terms & Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.

Cancellation of a Smartcard

All leavers must retain their NHS Smartcard if there is any possibility in the future that the user will access Spine enabled systems. Users that are leaving the NHS or Healthcare should have their access revoked by either cancelling or destroying the Smartcard or by closing the user.

Lost, Stolen and Damaged Smartcards

In the event a staff member has lost, stolen or damaged their Smartcard, they should report this immediately through the ServiceDesk and the RA will then follow the "Destroy Smartcard" process. The user must also register the incident on the **Datix** system so that it can be investigated, in line with Trust policy.

Sponsors and Smartcard Unlocking

The following options are available to Sponsors using the Care Identity Service (CIS)

- Raise and approve requests to assign a user to a position
- Directly assign a user to any assignable position

- Raise a request to register a new user
- Unlock smartcards & Renew certificates
- Assign users to workgroups

Additional guidance relating to sponsors can be found on the NHFT intranet:

http://thestaffroom.nhft.nhs.uk/clinical-systems

Safe Haven

The Trust operates Safe Haven procedures to maintain the privacy and confidentiality of person identifiable information held and transmitted. All employees are required to adhere to the NHFT Safe Haven procedures, the Trust procedure outlines:

- When a safe haven is required.
- The necessary procedures and requirements that are needed to implement a safe haven.
- Rules for different kinds of safe haven.
- Who can have access and to whom you can disclose information to.

Training requirements associated with this Framework

Mandatory Training

Information Governance training has been integrated into NHFT's induction programme for all new staff. For existing staff, an ongoing programme of refresher training will be delivered as part of NHFT's Information Governance work programme. Additional campaigns and awareness raising will be undertaken as appropriate.

Specific Training not covered by Mandatory Training

It is the responsibility of all managers to ensure attendance at induction and training programmes and to obtain feedback from staff regarding the knowledge and understanding they have obtained.

Individuals have an obligation to seek training, advice and support where uncertain in order to improve information practices appropriately.

Ad hoc training sessions based on an individual's training needs as defined within their annual appraisal or job description.

How this Framework will be monitored for compliance and effectiveness

This framework will be made available to the Public through the Trust Internet site in supporting documentation and upon application.

New employees will be made aware of this policy through the Induction process.

Information Governance activity will be reported monthly in Information Governance Highlight Reports to the Information Governance Group and the IMT Programme Board.

For further information

Please contact the Information Governance Team by emailing information.governance@nhft.nhs.uk

Equality considerations

The Trust has a duty under the Equality Act and the Public Sector Equality Duty to assess the impact of Framework changes for different groups within the community. In particular, the Trust is required to assess the impact (both positive and negative) for a number of 'protected characteristics' including:

- Age;
- Disability;
- Gender reassignment;
- Marriage and civil partnership;
- Race;
- Religion or belief;
- Sexual orientation;
- Pregnancy and maternity; and
- Other excluded groups and/or those with multiple and social deprivation (for example carers, transient communities, ex-offenders, asylum seekers, sex-workers and homeless people).

The author has considered the impact on these groups of the adoption of this Framework and identified that the advice and guidance service offered to patients and staff and reported IG incidents will be monitored.

Document control details

Author:	Information Governance Team
Approved by and date:	The Information Governance Planning Group Trust Policy Board – 25/06/2019
Responsible committee:	IM&T Programme Board
Any other linked Policies:	IGP107 – Health Records Management Policy
Framework number:	IGIS01
Version control:	V.3

Version No.	Date Ratified/ Amended	Date of Implementation	Next Review Date	Reason for Change (eg. full rewrite, amendment to reflect new legislation, updated flowchart, minor amendments, etc.)
V.1	06.07.2016	06/07/2016	01.07.2019	IGP101 has been reclassified as a procedure and has been reformatted in the new structure.
V.2	17/05/2018			The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union.
V.3	25/06/2019	26/06/2019	25/06/2022	Addition of a diagram showing IG Assurance Framework to reflect Data Protection Officer Role Addition of a Records Retention Section Expansion on the use of mobile devices.

Appendix A

Mobile Device Terms & Conditions

IT IS VERY IMPORTANT THAT YOU READ AND AGREE TO ALL OF THE FOLLOWING TERMS & CONDITIONS FOR USE OF THIS DEVICE:

This is an agreement between Northamptonshire Healthcare NHS Foundation Trust (NHFT) and the assigned user of this device.

Failure to comply with these terms and conditions may result in disciplinary action and removal of the device.

These terms and conditions cover the use of this specific device which is owned by Northamptonshire Healthcare NHS Foundation Trust (NHFT) and provided for the purpose of assisting/enabling you in your job role. Any additional device issued to you will require further agreement to these terms and conditions.

These terms and conditions apply to all staff members including permanent, temporary, contractors and volunteers.

You confirm that you will be the only user of this device, will not share it, or provide others with access to use unless has been approved by the Information Governance Team to do so. Where the use of this device is shared and has been approved by the Information Governance Team, as the asset owner you remain responsible for the use of the device and its security. Any member of staff allowing access to unauthorised persons deliberately or inadvertently may be subject to disciplinary action as per NHFT's disciplinary policy.

You agree that you will take all appropriate measures to protect the device and keep any stored information secure, further information is detailed in the Trust's IGIS01 Policy.

You must only save personal confidential data on the NHFT network drives provided. When working offsite you must use secure Virtual Private Network (VPN) access to enable this.

You must take appropriate precautions when using the NHFT device in public areas and be aware it is often not appropriate to do so. You must be aware of unauthorised persons being able to see the information on the screen and be sure to keep the information secure.

You must store mobile equipment securely when not in use on and off site.

You must ensure files containing personal or confidential data are adequately protected e.g. devices are to be encrypted and password protected.

You must only use NHFT approved removable media devices.

Any software and any data files created by you on NHFT mobile computer equipment is the property of NHFT.

You must immediately report if this device is stolen / lost to the IM&T Service Desk, inform your line manager and log it as an incident on Datix. Failure to report this may lead to disciplinary action as per NHFT's disciplinary policy.

The security of your mobile computer equipment is your responsibility;

This includes ensuring that this device is returned to the organisation if you are leaving employment (a final salary deduction may be made if equipment is not returned)

You must not disable the virus protection software or bypass any other security measures put in place by NHFT.

You must not remove personal information off site without authorisation.

You must not leave this device in places where it can be easily stolen.

You must not leave this device visible in the car when traveling between locations.

You must not leave this device in an unattended car.

You must not leave this device unattended in a public place.

You must not install unauthorised software or download software / data from the Internet.
You must not delay in reporting this device if it is lost or stolen.
All NHFT staff are bound by the same rules of confidentiality and security whilst away from their place of work as when they are at their desk.
If this device is reported lost or stolen, any information stored on the device will be remotely wiped and removed.
NHFT is able to lock this device remotely if required.
NHFT retains the right to put in place software restrictions remotely, in order that only approved applications can be used on the device.
NHFT will be able to remotely deploy applications and NHFT email accounts.
NHFT retains the right to be able to track the location of the device using GPS, Wi-Fi or 3G.
I CONFIRM THAT I AGREE TO AND ACCEPT THE TERMS AND CONDITIONS OF USING THIS DEVICE