

## Information Security Policy

Author:	Trust Data Protection Officer/Information Governance Manager
Sponsor/Executive:	Director of Finance (SIRO)
Responsible committee:	Information Governance Steering Group
Ratified by:	Business and Performance Committee
Consultation & Approval: (Committee/Groups which signed off the policy, including date)	Information Governance Steering Group, 10 February 2023
This document replaces:	4.0
Date ratified:	28 February 2023
Date issued:	28 February 2023
Review date:	28 February 2026
Version:	5.0
Policy Number:	CP08
Purpose of the Policy:	To provide an overarching framework to apply information security controls for Trust information and information systems
If developed in partnership with another agency, ratification details of the relevant agency	N/A
Policy in-line with national guidelines:	Yes



**Signed on behalf of the Trust:** .....  
**Anna Hills, Chief Executive**

Elizabeth House, Fulbourn Hospital, Fulbourn, Cambs CB21 5EF Phone: 01223 726789

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Comments</b>
1.0	June 2009	Information Governance Manager	Policy developed to comply with national requirements.
2.0	April 2011	Jason Clarke Information Governance Manager	Amended version to incorporate updated ASP procedures as present in the modified ASP IT Security Policy. Updated to add practical operational advice and guidance required by staff
3.0	April 2014	Kay Taylor Information Governance Manager	Amended version to incorporate instructions for bulk data transfers within emails, Personal devices connected to CPFT systems, confidential data and staff owned equipment. Mobile computer equipment abroad and encryption levels
3.1	January 2015	Kay Taylor Information Governance Manager	Additional paragraph added at 4.4, minor changes to duties of Trust Data Protection Officer/Information Governance Manager, addition of paragraph 6.6 Security of Information using Digital and Analogue Dictation.
3.2	December 2016	Kay Taylor Information Governance Manager	Additional paragraph added at 6.5 Security of Information when Mobile Working. Adjustment to paragraph 8 in line with Trust Mobile Device Policy. Addition of paragraphs 7.2 & 7.3 relating to access control.
4	May 2017	Kay Taylor Data Protection Officer/ Information Governance Manager	Changes to paragraph 7.1
5.0	January 2023	Richard Matt Associate Director of Business Technology & Kay Taylor Data Protection Officer/ Information Governance Manager	Paragraph amendments 6.5 7.1, 7.4, 9, new paragraph 11 and addition of Appendix A & B

## Contents

	Signed on behalf of the Trust: .....	1
1	Introduction .....	3
2	Purpose.....	3
3	Scope.....	4
4	Duties and Responsibilities .....	4
	4.1 Chief Executive .....	4
	4.2 Senior Information Risk Owner (SIRO) .....	4
	4.3 Data Protection Officer/Trust Data Protection Officer/Information Governance Manager .....	4
	4.4 Information Governance Steering Group .....	5
	4.5 Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) .....	5
	4.6 All Staff .....	5
5	Definitions .....	6
	5.1 Preserving.....	6
	5.2 The availability, .....	6
	5.3 Confidentiality .....	6
	5.4 And integrity .....	6
	5.5 Of the physical (assets) .....	7
	5.6 And information assets .....	7
	5.7 Of the Trust.....	7
	5.8 The ISMS.....	7
	5.9 Security Breach.....	7
6	Data Security.....	7
	6.1 Patient Identifiable Data (PID) .....	7
	6.2 Employees Data.....	8
	6.3 Business Confidential Data .....	9
7.	Exchanging Patient/Person Identifiable & Business Confidential .....	9
	<u>Data.....</u>	9
8.	Physical Security .....	11
	8.1 Security of data in transit .....	11
	8.2 Security of Information when Mobile Working .....	11
9	Network Security .....	12
	9.1 System Access Control.....	12

9.3	Access for Research Purpose .....	13
9.4	Documents used for Learning Purposes .....	13
9.5	Password Security .....	14
9.6	Account/Password Sharing .....	15
9.7	SMART Card Security.....	15
9.8	Data Storage.....	16
10	Computer Security .....	16
10.1	Software .....	17
10.2	Hardware .....	17
10.3	Physical Security in buildings .....	18
10.4	Modems, faxes and the NHS Code of Connection .....	18
10.5	Mobile Computing .....	18
11.	Cyber Security .....	20
12	Monitoring .....	20
13	Internet.....	21
14.	Incident Reporting.....	21
15	Non-Compliance .....	21
16	Education and Training .....	22
17	Monitoring Effectiveness of Implementation.....	22
18	Equality Impact Assessment .....	23
19	Links to Other Documents.....	23

## 1 Introduction

- 1.1 The Board and management of the Cambridgeshire and Peterborough NHS Foundation Trust (hereafter referred to as 'the Trust' or 'CPFT') are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the Trust in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and public image. Information and information security requirements will continue to be aligned with organisational goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.
- 1.2 In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Information Security Manual and are supported by specific, documented policies and procedures.

## 2 Purpose

- 2.1 The purpose of the Information Security policy is to help protect CPFT physical information from unauthorised disclosure whether by accident or deliberately, and to protect information systems from hazards and threats, and to ensure that the valuable information held in information systems is secure from accidental or deliberate unauthorised modification or disclosure.
- 2.2 CPFT's communications and computer systems are provided for business use and are to be operated and used accordingly.
- 2.3 Use of the Trust's computer systems are based on the following principles and this policy states staff responsibilities to abide by them:

**Confidentiality** - Access to information should be restricted to people who need to see it and are allowed to see it.

**Integrity** - Is the requirement to ensure that all system assets are operating correctly according to specification and therefore showing you the information as it was entered onto the system.

**Availability** - Is the requirement to ensure that information is delivered to the right person, in the right place, at the right time i.e. when and where it is needed.

### **3 Scope**

- 3.1** This policy is applicable to all areas of the Trust and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.
- 3.2** This policy is to be made available to all Trust staff and observed by all members of staff, both clinical and administrative.
- 3.3** The term 'staff' includes temporary employees, volunteers, third party service providers and contractors.
- 3.4** There will be a continuing professional development and educational strategy to accompany the implementation of this policy.

### **4 Duties and Responsibilities**

#### **4.1 Chief Executive**

The Chief Executive has overall responsibility for ensuring that appropriate arrangements and guidelines are in place for the use of information security within the Trust.

#### **4.2 Senior Information Risk Owner (SIRO)**

The Trust's Senior Information Risk Owner (SIRO) is the Director of Finance who is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for the Trust. Other responsibilities of the SIRO include:

- Ongoing development and day to day management of the Trust's Risk Management Programme for information, privacy and security
- Advise the Chief Executive and the Trust Board on information risk management strategies and provide periodic reports and briefings on Program progress

#### **4.3 Data Protection Officer/Trust Data Protection Officer/Information Governance Manager**

The Data Protection Officer/Trust Data Protection Officer/Information Governance Manager is the Owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements in the NHS Information Security Code of Practice. The Trust Data Protection Officer/Information Governance Manager will lead in the delivery of this approach reporting any risks that cannot be mitigated to the SIRO. The Trust Data Protection Officer/Information Governance Manager is also responsible for maintaining the Trust's Information Asset Register (incorporated into the Trust's Records of

Processing Activities) and working with IAO and IAA to ensure that risk assessments are conducted for assets and that the required controls are in place.

In addition the Data Protection Officer/Trust Data Protection Officer/Information Governance Manager will collate and review all Information Asset Owners annually assessed Information Asset registers on an annual basis and update the Trust Information Asset Register, ensuring that any unacceptable risks are included in the Trust Information Risk Register for review by the SIRO and Information Governance Steering Group.

#### **4.4 Information Governance Steering Group**

The Trust has established an Information Governance Steering Group, chaired by the Senior Information Risk Officer and includes the Trust's, Data Protection Officer/Trust Data Protection Officer/Information Governance Manager, the Trusts Associate Director of Business Technology, The Trust Associate Director of Information & Performance, SBS Information Security Manager the Trust Caldicott Guardian and other executives/specialists/risk specialists to support the ISMS framework and to periodically review the security policy.

#### **4.5 Information Asset Owners (IAOs) and Information Asset Administrators (IAAs)**

Trust Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) shall ensure that information risk assessments are performed at least once each year on all information assets where they have been assigned 'ownership', following guidance from the Trust Data Protection Officer/Information Governance Manager on assessment method, format, content, and frequency. Information Asset Administrators IAOs shall share the risk assessment results by exception if the risk level is assessed as severe and will submit associated mitigation plans to the Trust Data Protection Officer/Information Governance Manager for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks. It is expected that the IAO and IAA will monitor and manage the access controls to key information assets.

#### **4.6 All Staff**

Information Security is the responsibility of all Trust employees. All employees are therefore required to highlight any breaches they come across or are made aware of via the Trust's incident reporting tool.

All employees of, or working on behalf of, the Trust are expected to comply with this policy and with the ISMS that implements this policy.

In particular, all Directorate/Departmental and Service Managers are responsible for ensuring the correct and consistent implementation of this policy within their respective service areas.

## **5 Definitions**

In this policy, “information security” is defined as:

### **5.1 Preserving**

This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in the Security Manual) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the Trust’s disciplinary policy. All staff will receive information security awareness training and more specialised staff will receive appropriately specialised information security training.

### **5.2 The availability,**

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient, and the Trust must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans in place to continue those activities identified as critical in the event of disruption.

### **5.3 Confidentiality**

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to the Trust’s information and proprietary knowledge and its systems including its network(s), website(s), extranet(s), and e-commerce systems.

### **5.4 And integrity**

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing

deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency (including for network(s), e-commerce system(s), web site(s), extranet(s) and data back-up plans, and security incident reporting. The Trust must comply with all relevant data-related legislation in those jurisdictions within which it operates.

## **5.5 Of the physical (assets)**

The physical assets of the Trust including but not limited to computer hardware, data cabling, telephone systems, filing systems and physical data files.

## **5.6 And information assets**

The information assets include information printed or written on paper, transmitted by post or shown in visual and audio recordings, or spoken in conversation, as well as information stored electronically on any medium and information transmitted electronically by any means. In this context “data” also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

## **5.7 Of the Trust**

The Cambridgeshire and Peterborough NHS Foundation Trust and such partners that are part of our integrated network and have signed up to our security policy.

## **5.8 The ISMS**

**ISMS** is the Information Security Management System, of which this policy, the information security manual and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO 27001 and ISO 27002 information security standards.

## **5.9 Security Breach**

A **security breach** is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the Trust.

# **6 Data Security**

## **6.1 Patient Identifiable Data (PID)**

## **What is PID?**

Patient Identifiable Data is information that allows the identification of an individual patient to be revealed, either explicitly or by implication. It includes:

- Patient's name, address
- Full post code
- Pictures, photographs, videos, audiotapes or other images of patients
- Any grouping term such as 'baby', 'new-born baby'
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

The Trust does not consider local patient identifiers such as system unique identifying numbers as patient identifiable information, PID extends only to data that if found by a wrongdoer could be used to identify a person somehow.

## **Sharing patient information**

Patient identifiable data must not be shared with or made accessible to people who are not authorised to see it.

Only staff, which as a result of their tasks requires access to patient identifiable data, should be allowed to access such data. Whenever possible, patient data should be anonymised.

## **Identifiable patient information**

The number and type of health and social care related data items, which could allow identification of an individual, should be reduced to the minimum essential for the purpose if not anonymised.

## **Access limitations principles**

There should be locally agreed arrangements for ensuring that patients are personally made aware of the purposes to which information about them may be accessed, as well as ways in which they can exercise choice.

## **6.2 Employees Data**

Employee files also contain personally identifiable data and must be kept in accordance with the UK GDPR & Data Protection Act. It is the Manager's responsibility to ensure that electronic and paper records are

securely saved/stored. This information must be stored in a locked filing cabinet with controlled and limited available access or saved in an electronic file with restricted access. Personally identifiable data must not be shared with individuals other than when strictly necessary; should be available for access only to those on a need to know basis; and should not be left unattended, such as on a desk.

### **6.3 Business Confidential Data**

#### **What is Business Confidential Data?**

In general terms, business confidential data includes any information that is not available to the public. Data that is highly confidential is information that would damage the organisations' business if it became known to a wider public base.

Confidential data is one of the Trust's most valuable assets. If that information becomes public, it may affect the organisation's competitiveness and put at risk the livelihoods of you and all of your colleagues.

### **7. Exchanging Patient/Person Identifiable & Business Confidential Data**

Exchange of data between organisations must be controlled.

#### **Email**

All Emails sent to and from health and social care organisations must meet the secure email standard (DCB1596) so that everyone can be sure that sensitive and confidential information is kept secure.

You can now send emails securely between your CPFT.nhs.uk and NHS.Net addresses.

Trust employees must not send personal, sensitive, or confidential information to a non-secure email address unless it is encrypted. Information sent to Service Users containing personal information must be sent in a word document that is password protected with the password sent separately. (Using the patients date of birth in the format DDMMYYYY).

To send an encrypted email message, prepend [SECURE] to the subject line of the email – Where patients are unable to receive encrypted messages this must be agreed by a line manager and personal information must still be password protected in a word document.

More information can be found in Appendix 4. Full details can be found in the Trust Electronic Communications Policy

Extreme care must be taken to ensure that your email is addressed to the intended recipient.

All employees need to be aware that the Trust can monitor the use of email facilities for the following reasons:

1. To ensure compliance to this policy.
2. To protect the organisation from a host of legal liabilities including harassment and discrimination in the workplace, defamation, transmitting of confidential information.
3. To guard against inappropriate and excessive personal use.

For further information please see the Trust Electronic Communications Policy

### **Disclaimers**

The use of email disclaimers are recognised as good practice but are not legally binding. Should you wish to use an email disclaimer please follow your own organisations' guidelines on style and wording

### **Removable Media**

If files are copied to transportable media such as CD/DVDs (for exchange between organisations) then they must be encrypted. For help and advice on encryption methods contact the CPFT Business technology team.

### **Encryption Standards**

When storing or transmitting data it must be encrypted (minimum AES-256) to make sure data can only be accessed by authorised users. Typically, this means a password is required to 'unlock' the data.

Your encryption should include:

- full disk encryption so that all data is encrypted
- file encryption so that individual files can be encrypted
- an encryption password that is a mix of upper and lower case, numbers and special characters (i.e. #, & !) and is kept secret
- (where possible) password protection to stop people making changes to data

For help and advice on encryption methods contact the CPFT Business Technology team.

## **8. Physical Security**

### **8.1 Security of data in transit**

If copies of data need to be transported between sites on physical media, then organisationally approved secure couriers must be used.

A secure courier is not an internal post service or member of staff who happens to be visiting a location for some other purpose. A secure courier will be able to provide adequate security assurances (set out in a written contract) and a tracked mode of collection and delivery.

The Trust utilises various technologies to ensure sensitive data is encrypted during transit. These include, but are not limited to, virtual private networking (VPN) for remote connectivity, Transport Layer Security (TLS) for secure email transport, Secure Socket Layer Transport (SSL) and others.

### **8.2 Security of Information when Mobile Working**

Community based health staff must transport **all** Trust Information) in A3 size red bags available via e-procurement. Seals must also be used to ensure bags are locked.

All other agile working staff must transport Trust information in a lockable secure document case/wallet.

The use of printed documents when outside of Trust premises must be kept to only the minimum required in order to perform work safely when agile working and should be filed or destroyed securely back at base as soon as possible. Consider how you can minimise the need to carry paperwork for example using your Trust issued mobile phone to photograph a visit list.

Trust information and Equipment must be locked in the boot of the car out of sight if it is necessary to be left unattended. No Trust Information or Equipment must be left over night in a car boot. It must be locked away securely at home.

### **8.3 Security of Information for Office Based and Home Working staff**

Paperwork must never be left unattended and should be locked securely away when not in use at all times.

The “control, Alt, delete” function must be used if you are leaving your laptop/PC unattended for any period of time, and you must log out completely when finishing your work.

Avoid leaving the mobile device within sight of ground floor windows or within easy access of external doors.

Ensure that your computer and related media and agile devices are physically secure.

Keep technology out of public view where possible; use blinds, keep doors closed etc. Lock office doors when computers are left unattended.

Keep removable media - CDs, DVD's, USB memory sticks – locked out of sight.

Where computers are used in public areas, make sure the screen cannot be viewed by members of the public, except where this is a requirement for this e.g. touch screens for patient use

#### **8.4 Security of Information Using Digital/Analogue Dictation**

- Recordings must be made in a confidential environment to ensure sensitive/private information is not overheard.
- If you are making a voice recording of another person they must be informed of your intention and consent gained before this can commence.
- When dictating personal or sensitive personal information the minimum identifiable data must be used e.g. the initials, NHS number and DoB.
- Ensure transcription is done using headphones in order to protect confidentiality
- The recording must be erased immediately the transcription has been completed and approved

### **9 Network Security**

#### **9.1 System Access Control**

System access must be authorised by your line manager or the appropriate Information Asset Owner (IAO).

System privileges and access rights will be allocated on the basis of your specific role requirements; they are not based on the status of your role.

System usernames and passwords that are allocated to you, are your responsibility and for your use only.

Never share your system access account with anyone else. If someone else logs in as you, whatever they do will be registered against your name and you will be held responsible.

Never use someone else's system access account.

Ensure that PCs/terminals are logged off when left unattended or lock the screen by invoking the screen saver using the CTRL-ALT-DELETE keys and select 'Lock Computer'.

All detected unauthorised attempts at system access must be notified to the SBS ICT Service Desk. SBS will notify all incidents to The Trust's IT management for investigation. The Trust's IT Management must ensure that the organisation's IG lead is informed to facilitate any required investigation.

## **9.2 System Access Control non NHS Organisations for Audit Purpose**

Non NHS organisations may have a requirement to access Trust systems for Audit purposes in support of patient care, and in these cases may require access to clinical information.

Requests in these instances for access to Electronic patient record systems must be submitted with the justification for the access requirement to the Trust Data Protection Officer/Trust Data Protection Officer/Information Governance Manager.

All non NHS organisations will be required to sign security and confidentiality agreements with the Trust.

External organisations will only be allowed access to specific/relevant systems relating to their functions.

## **9.3 Access for Research Purpose**

Research within the NHS relies on working in partnership with the Higher Education sector and is often undertaken by non-NHS staff, including staff employed by Higher Education Institutions (HEIs). access requests for research purposes must be directed to the Research and Development Team

## **9.4 Documents used for Learning Purposes**

On occasions where staff members are legitimately permitted to use existing physical patient documents for learning purposes this must be authorised by the appropriate Line Manager and the document must be completely anonymised prior to being issued.

## **9.5 Password Security**

Password Security is the responsibility of the individual. You are accountable for system activity under your username

Never share your password with anyone else.

Never write your password down.

For security reasons, most systems will require you to change your password periodically. However if you feel your password may be compromised, do not wait until the system asks you to change it, do so immediately.

When allocated a new password (either when your account is first issued to you or following a change of password at a later date) most systems will immediately require you to change it. If the system does not force a password change immediately, then manually change the password as soon as possible. Do not continue to use the password that has been allocated to you.

Passwords should be formulated in such a way that they are easily remembered but difficult to guess. Passwords should not relate to the system, or the user e.g. do not use well known family or pet names. A balance between usability and security is best.

Passwords must consist of a minimum of 8 characters, but for improved security they should include upper and lower case surface mail, plus numeric and/or special characters where the system allows. The Trust utilises "Password phrases" for the purpose of ICTS access.

In exceptional circumstances, where authorised by your organisation, generic accounts may be set up for specific purposes. These account details must only be shared with authorised members of staff, and the password must not be written down for all to see e.g. on a post-it note, taped to the base of removable media etc.

If access to another user's mailbox or personal drive is required in circumstances where absence from work is unexpected e.g. sick leave, personal emergencies etc. and there is an immediate business need to have access to this information, then this access must be authorised by the employee's Director.

## **9.6 Account/Password Sharing**

If it is discovered that a member of staff is sharing their account and password phrase details, the account(s) in question will be disabled. The incident will be reported to the organisation's Trust Data Protection Officer/Information Governance Manager.

The account will only be re-enabled when authorisation to do so is received via email from the relevant organisation's Information Governance Manager (or another member of senior management).

Sharing passwords/password phrases, and logging onto the network as another individual is a breach of this policy and may lead to disciplinary action being taken against you. (See section 12 on Non-Compliance.)

## **9.7 SMART Card Security**

SMART cards are issued to staff to provide access to NHS national applications. Through SMART card access individuals are enabled to access personally identifiable patient or personnel data which is extremely sensitive and confidential in its nature.

- They are issued on an individual basis and remain the responsibility of that individual.
- Never share your SMART card or PIN with anyone.
- Never allow another member of staff to use the system while you are logged in with your SMART card.
- Never use the system while someone else is logged in with their SMART card.
- Never write your PIN down nor stick it to your SMART card.
- Never leave your SMART card in the card reader when it is not in use.
- Always store your SMART card in a secure place – do NOT leave it lying around.
- If your SMART card is lost or stolen report it to your line manager and the SBS ICT Service Desk immediately.

Where national applications have Role Based Access Controls (RBAC) or Position Based Access Controls (PBAC), legitimate relationships are created through RBAC and patient consent. The Trust will receive

reports detailing user access to records where there is no apparent legitimate reason to do so. These reports will be investigated by your organisation to establish if the access was appropriate. Inappropriate access may result in disciplinary action.

## **9.8 Data Storage**

Various network drives are provided to enable staff to store data securely. The data on these drives is backed up on a daily basis.

### **Personal Drive**

Your personal drive e.g. P:\ is provided to enable you to save work related files that pertain only to yourself e.g. HR or appraisal related documents. This area is not provided for storing personal data e.g. photographs of family and friends, music files etc.

### **Shared Drive**

The shared drive e.g. S:\ is where any non-confidential work related files should be saved. This area should contain files which it would be appropriate to share across departments or directorates.

### **Restricted Drive**

The restricted drive e.g. R:\ is for saving any confidential work related files. This will contain files that should only be seen by a limited number of staff e.g. within a small team, a manager & PA etc., and where it would not be appropriate to save them on the Shared drive.

### **MSOffice SharePoint/Teams Access**

Access must be restricted in the same way as it would be to the R Drive, *“Access is on a Need to Know basis only”* Further guidance on the use of MS Office and security are available on the Trust Digital Ambassador SharePoint Pages.

### **Local Drive**

In some circumstances staff may have access to their local drive e.g. C:\.

Never save confidential work related files on the local drive of a PC as this is restricted and cannot be accessed by other staff when required.

## **10 Computer Security**

## 10.1 Software

Users must take all reasonable steps to protect against the installation of unlicensed or malicious applications

Commercial software (including shareware) must have a valid license for each prospective user, and must be validated, approved and installed by CPFT business Technology Team.

All software on the device must either be provided and installed by SBS IT or approved by Cambridgeshire and Peterborough NHS Foundation Trust for installation by the user. Users should understand that unmanaged or unapproved installations compromise the operating environment and also constitute a security risk, including the intentional or unintentional spreading of software viruses and other malicious software.

Staff are not authorised to install any software to their work computer – whether desktop or mobile device. This includes software downloaded from the Internet as well as software on physical media.

Software must also be removed by SBS ICT staff, to ensure that it is uninstalled correctly, and to enable licensing records to be maintained. If you require software uninstalling please contact the SBS ICT Service Desk.

Non-NHS procured software will not be installed onto an organisation's computer equipment.

Software obtained illegally will not be installed onto an organisation's computer equipment.

Any and all instances of unauthorised installations of software will be reported to the staff member's organisation.

## 10.2 Hardware

All computer equipment must be authorised by the Trusts Associate Director of Business Technology or a Senior Director and procured through the SBS Purchasing Department. Non-NHS procured and/or personal computer equipment must not be connected to the organisation's network. Non-NHS procured and/or personal computer equipment will not be supported by SBS.

Personally owned mobile phones/Dictation Devices not sanctioned for business use by the Trusts Head of IT, a Senior Director or SBS IT must not be connected to the organisations private network

The organisation's computers are provided as tools for you to do your job; they do not act as a personal computer. They are subject to security controls, and they cannot be treated in the same way as your PC at home.

### **10.3 Physical Security in buildings**

All members of the ICT department are issued with ID cards and must carry them at all times. Do ask them to produce their ID card if you are unsure as to their identity, before you allow them to access or remove your computer.

Request anyone not displaying an ID badge in non-public areas to produce their ID or visitors badge.

### **10.4 Modems, faxes and the NHS Code of Connection**

New HSCIC Guidance has devolved Fax and Modem connectivity to local IG Control. Requests for connecting Devices containing modems to local area networks (LANS) must be directed to the SBS IT Help Desk.

### **10.5 Mobile Computing**

This section covers:

- Portable Computers (Laptop and Tablets)
- Smart Phones
- Remote Access (RAS) / VPN Tokens

Only mobile devices authorised by the Trusts Associate Director of Business Technology or a Senior Director and procured through the SBS Purchasing Department must be used by staff. Personal mobile computing devices must not be used for business purposes and must not be connected to the NHS network.

Mobile computers/phones must not be taken abroad without prior permission from the line manager/budget holder, approval must be documented.

The saving, copying and storage of person identifiable or confidential data on staff personally owned equipment is strictly forbidden. Staff may only use Trust supplied and encrypted machines and Trust supplied encrypted USB data sticks to store NHS data.

The only exception whereby personal devices can be used for business purposes is when you have been authorised to use the 'work from

home/secure desktop' solution. To maintain security, this solution can only be used in conjunction with an SBS VPN token. Synchronisation will only be supported between a SBS procured or other authorised mobile device and the member of staff's NHS email account.

All mobile devices must have their storage drives encrypted. If you have any concerns please contact the SBS ICT Service Desk.

Never save person identifiable data (PID) on your mobile computing device e.g. the C:\ drive of your laptop.

Mobile computer security is your responsibility at all times.

Never leave the mobile computing device unattended in work premises or in a public place.

All mobile computing devices must be securely locked away when not in use.

Ideally mobile computing devices should not be left in your car. However, if doing so is unavoidable, never leave the mobile device in view in the inside of your car - lock it away in your car boot and remove at night.

Portable devices (e.g. laptops/Tablets and notebooks) need to receive updates e.g. anti-virus and Windows updates, on a very regular basis. To facilitate this, your device needs to be connected either to the organisation's network or the Internet (via your broadband connection at home) frequently.

Never write down passwords and store them with the mobile device.

Damaged or broken mobile devices must be returned to the SBS ICT department before being sent for repair, to ensure that the device is reimaged/erased by an SBS ICT engineer, and any data is removed. If the device cannot be repaired then it must be disposed of in accordance with the Disposal of IT Equipment policy and WEEE regulations (Waste Electrical and Electronic Equipment Directive).

All mobile computer devices must be returned to your manager if they are no longer required e.g. following a change of post, leaving the organisation etc.

Further details on management of mobile devices can be found in the Trust Mobile Device Policy.

## 11. Cyber Security

All staff must be aware of the threats to security of patient, business and personal confidential information via Social Engineering ( the art of manipulating people so they give up confidential information). Typical ways of this being perpetuated are via:

- Phishing and spear- phishing attacks
- Smishing
- Voice Scams
- Remote Access Attacks (RAT)

### Emails

If you receive an email to your Organisational email address that looks suspicious due to:

- Grammatical errors or irregularities
- Odd hyperlinks
- Creating undue time pressures on you to respond

Do not respond or click on the hyperlink forward it immediately to the SBS Help Desk.

### Voice calls

If you get a call and you are unsure if it is genuine:

- hang up and ring the organisation back , don't use the number provided by the caller, find the number yourself
- Don't reveal personal confidential information relating to patients, staff or the business unless you are sure that they are legitimately entitled to the information, and you are authorised to give that information.

## 12 Monitoring

The Trust Information Security & Confidentiality Audit procedure outlines the arrangements adopted by CPFT for the auditing and monitoring of data security, protection, and confidentiality issues in relation to the processing of personal data. It provides an assurance mechanism by which the effectiveness of controls implemented within the organisation are audited, areas for improvement and concerns are highlighted together with recommendations to ensure information security and confidentiality is maintained. To ensure access to health records is legitimate Privacy Audits are conducted for records held in both SystemOne and the Summary Care Record.

The full Procedure can be found at Appendix A of this policy

## **13 Internet**

It is recognised that access to the Internet is a useful means of communication, a valuable resource and essential to support NHS business.

The Internet is primarily for business use. Employees are permitted to use the Internet for occasional and reasonable personal use, subject to the terms outlined in the Trust's Internet Acceptable Use Policy.

Occasional and reasonable personal use of the Internet is a benefit and not an entitlement. This benefit may be withdrawn at any time, for either a specific individual or for all employees of the organisation. Employees will be informed prior to access being revoked.

For further information please see the Internet Acceptable Use Policy.

## **14. Incident Reporting**

**14.1** All incidents that constitute a loss of hardware or data, which could potentially lead to a breach of confidentiality (whether patient, personnel or business), must be reported. All information security/cyber security incidents are to be recorded on Datix, which is the Trust's incident reporting system.

**14.2** The organisation's Trust Data Protection Officer/Information Governance Manager will instigate investigation procedures to try and establish the nature and potential threat of the incident and advise the organisation on recommended action.

**14.3** Incidents could involve:

- Theft or loss of hardware
- Theft or loss of software or data
- Unauthorised or malicious alteration of data
- Unauthorised system access
- Password sharing
- Misuse of system/privileges
- Illegal software download
- Virus attack

## **15 Non-Compliance**

**15.1** Any breach of this policy can result in disciplinary action being taken against you, up to and including your dismissal, in line with the Trust's Disciplinary Policy.

**15.2** Non-compliance can also damage the reputation of the organisation and open the organisation and individual to a host of legal liabilities.

**15.3** If further clarification is required please, in the first instance, contact your manager. For further advice and assistance contact the Trust's Trust Data Protection Officer/Information Governance Manager and/or Human Resources Department.

## **16 Education and Training**

**16.1** Information security, IT security and technical support staff will receive specific training, as will the incident response team.

**16.2** All employees will receive security awareness training as part of the mandatory induction training and were identified as a requirement.

## **17 Monitoring Effectiveness of Implementation**

### **17.1 Process for Monitoring Compliance and Effectiveness**

The Information Governance Steering Group will retain responsibility for the ongoing review and update of this policy.

Information Security breaches will be reported through Datix (see Section 11).

The implementation of the policy will be audited as part of the annual Data Security and Protection Toolkit review.

Internal audit review will be used to measure Trust compliance with the Data Security & Protection Toolkit and Trust implementation of the Information Security policy.

### **17.2 Standards/Key Performance Indicators**

The Trust will hold and maintain an overall information asset register Information governance risks will be included as part of the Trust's Risk Register.

Information security will be included in the Corporate Induction programme on Information Governance.

Information security leaflets are available to all staff via the Trust Information Governance intranet page which outlines individual responsibilities.

The Information Governance Steering Group will routinely review information security incidents.

## **18 Equality Impact Assessment**

**18.1** This policy has been subjected to an Equality Impact Assessment and is not considered to have a discriminatory impact on any individual or groups.

## **19 Links to Other Documents**

### **19.1 Related policies/guidelines**

- Information Governance Policy.
- Data Quality Policy
- Data Protection and Access to Records/CCTV policy.
- Electronic Communications Policy
- Internet Acceptable Use Policy
- Freedom of Information Act policy.
- Information Risk Policy
- Professional codes of conduct from the BMA, GMC and NMC and others including Allied Health Professionals, Finance Professionals and NHS Managers.
- Clinical Record Keeping Policy.
- Research Governance policy.
- Safe Haven policy.
- CPFT Access Control Policy
- Records Management Policy

### **19.2 Related legal and regulatory requirements**

- Data Protection Act 2018.
- UK General Data Protection Regulation
- Human Rights Act 1998.
- Freedom of Information Act 2000.
- Access to Health Records Act 1990.
- Computer Misuse Act.
- Copyright, designs and patents Act 1988 (as amended by the copyright
- Computer programmes regulations 1992).
- Crime and Disorder Act 1998.
- Electronic Communications Act 2000.
- Regulations of Investigatory Powers Act 2000 (RIPA).
- Mental Capacity Act 2005.

### **19.3 Supporting documents**

- Information Security Management: NHS Code of Practice April 2007.
- UK Strategy for Information Assurance:
- Protecting our information systems CSIA Cabinet Office 2004.
- Lord Chancellor's code of practice on the management of records under section 46 of the Freedom of information act 2000 - November 2002

Appendix 1

**Information Security  
&  
Confidentiality Audit Procedure**

<b>Target Audience</b>	<b>CPFT Staff</b>
<b>Approving Committee</b>	<b>Information Governance Steering Group</b>
<b>Date Approved</b>	<b>February 2022</b>
<b>Last Review Date</b>	-
<b>Next Review Date</b>	<b>January 2023</b>
<b>Procedure Author</b>	<b>Data Protection Officer</b>
<b>Version Number</b>	<b>V1</b>

CPFT is committed to an environment that promotes equality, embraces diversity, and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via CPFT's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

## Version Control Sheet

Version	Date	Author	Comment
1	January 2023	Data Protection Officer	For approval by Information Governance Steering Group

DRAFT

## Contents

1	Introduction .....	<b>Error! Bookmark not defined.</b>
2	Purpose.....	<b>Error! Bookmark not defined.</b>
3	Aims and Objectives .....	<b>Error! Bookmark not defined.</b>
4	Roles and Responsibilities .....	<b>Error! Bookmark not defined.</b>
5	Definitions .....	<b>Error! Bookmark not defined.</b>
6	Monitoring and Auditing Access to Confidential Information.....	<b>Error! Bookmark not defined.</b>
7	Management of Incidents.....	<b>Error! Bookmark not defined.</b>
8	Providing Audit Information To Patients/Service Users.....	<b>Error! Bookmark not defined.</b>
9	Confidentiality & Information Security Incident Reporting.....	<b>Error! Bookmark not defined.</b>
10	Training and Awareness.....	<b>Error! Bookmark not defined.</b>
11	Monitoring and Review.....	<b>Error! Bookmark not defined.</b>
12	Legislation and related documents.....	<b>Error! Bookmark not defined.</b>
	Appendix A - Data Security / Confidentiality Audit (Observational on site ).....	
	Appendix B – Privacy Officer Electronic Record Audit.....	

DRAFT

## **1. Introduction**

Cambridgeshire & Peterborough NHS Foundation Trust (CPFT) is committed to a programme of effective information risk and incident management incorporating data security, protection, and confidentiality. Access to personal confidential information must be in accordance with UK Data Protection legislation, more specifically the UK General Data Protection Regulation (GDPR) principles and within the jurisdictions permitted for a Health and Social Care Organisation.

The UK GDPR is a legal framework that protects individual's personal data. For CPFT staff to process this type of information there must be a legal basis as per UK GDPR and access must be on a need-to-know basis, justified when required and monitored. CPFT are therefore required to regularly review how CPFT staff process personal data.

## **2. Purpose**

This procedure outlines the arrangements adopted by CPFT for the auditing and monitoring of data security, protection, and confidentiality issues in relation to the processing of personal data. It provides an assurance mechanism by which the effectiveness of controls implemented within the organisation are audited, areas for improvement and concerns are highlighted together with recommendations to ensure information security and confidentiality is maintained.

CPFT has a procedure for investigating personal data breaches of data security and confidentiality as documented in the Incident Management Policy including Serious Incidents & Near Misses.

This procedure applies to all CPFT staff, as well as those who work on behalf of CPFT, such as third-party contractors and others (e.g. business partners, including other Public Sector bodies, volunteers, commercial service providers etc.).

## **3. Aims and Objectives**

Data security, protection and confidentiality audits will focus on control within electronic records management systems, paper record systems and data security and confidentiality processes undertaken by departments, for example checking transfers of information processes and housekeeping, such as screen locking and ensuring confidential information is not left unattended. The purpose is to determine whether data security and / or confidentiality has been put at risk or breached through deliberate or perhaps unknown misuse of systems because of weak, non-existent, or poorly applied controls.

Assurance that controls are working should be part of CPFT's overall information risk assurance framework. Failure to ensure that adequate controls to manage and safeguard data security and confidentiality are implemented and fulfil their intended purpose may result in a breach of that confidentiality. This potentially could contravene the requirements of Caldicott Principles, the UK General Data Protection Regulation (UKGDPR), the Data Protection Act 2018, the Computer Misuse Act 1990, and the Human Rights Act 1998.

#### **4. Roles and Responsibilities**

##### **Caldicott Guardian & Senior Information Risk Owner (SIRO)**

The SIRO and Caldicott Guardian will be informed where serious breaches occur. They will also be updated with the findings of any confidentiality audits and ensure that appropriate action is taken. The Caldicott Guardian will also be responsible for ensuring that access to personal confidential information remains relevant and is regularly audited within the Trust.

##### **Information Governance (IG) Team**

The Information Governance Team, led by the Data Protection Officer/Information Governance Manager, are responsible for co-ordinating the approach for investigating data security and confidentiality alerts which arise from incidents, complaints, audit reports, informal alerts. The IG Team will provide a comprehensive audit report from their findings. This will be circulated to CPFT's Information Governance Steering Group (IGSG). Through this route, issues will also be raised with the Trust Board through the regular reporting of Minutes and activities from IGSG to the Board's Business & Performance Sub-Committee.

##### **Information Asset Owners (IAO)**

The Information Asset Owners (IAOs) support the SIRO and will support the IG team when areas of concern relating to information risk are identified within their department.

##### **Privacy Officers**

The nominated Privacy Officers for the SystemOne Units and Summary Care Record will be responsible for investigating alerts and submitting a report of the findings on a monthly basis .

#### **5. Definitions**

##### **General Data Protection Regulation 2016 (GDPR)**

The GDPR is Data Protection legislation. The aim of the GDPR is to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and the rules enabling the free movement of personal data.

## **Processing**

This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

## **Personal Data**

This contains details that identify individuals, even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

## **Business Sensitive Information**

This is information that if disclosed could harm or damage the reputation or image of an organisation.

## **Personal Data Breach**

As per Article 4(12) of the GDPR, a “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

## **Information Risk**

An identified risk to any information asset that CPFT holds. Refer to the Trust Information Risk Policy for further information.

## **6. Monitoring and Auditing Access to Confidential Information**

In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis. This will be achieved by putting in place arrangements for both proactive and reactive auditing of access to personal confidential information, testing staff understanding via awareness surveys and observations the results of which will be reported on and communicated to all staff.

The Data Security & Protection Toolkit (DSPT), which is completed annually to demonstrate CPFT's compliance with the UK GDPR, may contain staff survey questions. When provided, the IG Team will ensure the survey is circulated to CPFT to assess IG comprehension. This assists to highlight areas of good practice and identify areas where further training / guidance / support are required.

## **Proactive Monitoring**

### **Auditing Access to Electronic Records**

This will be achieved for systems where an automated function exists for the alerting of user access to records for subsequent review by someone with Privacy Officer Functions within the system. Examples of proactive monitoring on systems accessed by CPFT staff include:

- Summary Care Record (SCR)
- SystemOne
- PCMIS

These systems generate alerts when users access or override one of the information governance controls in place.

The alerts will prompt the receiving staff member to establish if the access was justified or potentially inappropriate, which will warrant further investigation.

An agreed sample size of alerts will generally be reviewed on a monthly basis in line with the SCR/CRV Investigation Process. [Information governance for Summary Care Records \(SCR\) - NHS Digital](#)

Privacy monitoring tools will also be used for proactive monitoring of user access to health records and systems, the monitoring tools will review user access to identify suspicious and potentially inappropriate patterns of access for further investigation by the Information Governance department. The outcome of these reviews will be escalated for further investigation as appropriate. Findings will be reported back via the Information Governance Steering Group on a quarterly basis as an agenda standing item.

The methodology for the investigations are contained in Appendix B

### **Confidentiality Observations**

Annual Confidentiality Observations will be conducted by the IG team and Team Leaders and where trends are identified unannounced observations maybe undertaken, and will cover the following areas:

- Audit and observations of any data security, confidentiality, or information security breaches
- Security applied to manual files e.g. storage in locked cabinets / locked rooms
- The use of and disposal arrangements for post-it notes, notebooks and other temporary or paper recording material
- Retention and disposal arrangement – confidential waste procedures / archiving procedures
- The location of post trays for incoming and outgoing mail – are they located in secure areas
- Staff comprehension regarding their responsibilities pertaining to data security and confidentiality and the rights regarding access to confidential information
- Checks to test staff awareness regarding:
  - Right of Access / Subject Access requests
  - Freedom of Information requests
  - how to report data security / IG incidents
  - Who are the key IG contacts
  - What is personal data and a personal data breach
  - Observations of good practice regarding assuring the data security and confidentiality of personal data and business sensitive data

## **Reactive Monitoring**

Reactive confidentiality audits will generally fall into 2 scenarios:

1. Where misuse of system access is alleged in relation to privacy/confidentiality breaches.
2. Where evidence is required to support management's concerns/investigations about staff conduct, e.g. excessive use of the Internet, email activity or conduct (where the primary concern is not about a breach of privacy/confidentiality, however the audit information may have privacy implications).

This procedure addresses audit requests where privacy/confidentiality breaches are reported or suspected; and procedures for conducting audits in relation to staff conduct, management concerns/ investigations will also be covered under the relevant policies (i.e. the Information Security & Risk Policy, Email Policy).

## **Methodology**

Confidentiality observational checks are undertaken using a variety of methods such as unannounced spot checks and annual observations conducted by the IG Team and/or Team Leaders using the methods as listed in Appendix A. The

results of the observations are discussed at the Information Governance Steering Group and any non-compliance will be followed up.

Where non-compliance and / or information risks are observed, this will be reported back to the relevant line manager and include recommendations for action and a target date for completion. A named individual (such as Line Manager / Information Asset Owner) will be responsible for ensuring that the recommendation is implemented. Further checks will be made to ensure the recommendation has been implemented and risks mitigated

## **7. Management of Incidents**

The IG Department monitors IG-related incidents logged in DATIX and will follow up all IG incidents to achieve a satisfactory outcome in liaison with investigating managers. More serious incidents are managed using the Trust's Incident Reporting Policy and Procedures and IG Serious Incident Reporting Investigation (SIRI). All IG incidents are reported to the IG Committee, which will escalate any unsatisfactory outcomes to the Senior Management Team and communicate pertinent IG issues/messages to staff using, for example, Trust Briefing and intranet notice board bulletins.

## **8. Providing Audit Information To Patients/Service Users**

Both the National Information Board in 'Personalised Health and Care 2020' and Dame Fiona Caldicott in the 'Report of the Caldicott2 Review' have reaffirmed the commitment made in the NHS Care Record Guarantee to ensure that a record of who has accessed a service user's health records can be made available in a suitable form to service users on request. All requests of this nature need to be directed to the Information Governance Team

## **9. Confidentiality & Information Security Incident Reporting**

Actual or potential breaches of confidentiality and information security must be reported **immediately** on Datix. Please contact the Information Governance Team at [informationgovernance@cpft.nhs.uk](mailto:informationgovernance@cpft.nhs.uk) for guidance if required on how to do this. The IG Team will then review the incident and ensure remedial action is taken to mitigate further breaches. The Data Protection Officer will ensure the incident is reported to the ICO if required, via the Data Security and Protection Toolkit (DSPT).

The procedure for reporting incidents is contained within the Trust's Incident Management Policy including Serious Incidents & Near Misses

The Data Protection Officer is responsible for ensuring the Caldicott Guardian and / or SIRO are informed of any concerns highlighted as a result of monitoring compliance with data security and confidentiality processes.

If any member of staff fails to adhere to data security and confidentiality processes this will be dealt with in accordance CPFT's Disciplinary Policy.

An Information Governance Confidentiality/Information Security report is submitted to the Information Governance Steering Group for review and discussion.

## **10. Training and Awareness**

This procedure will be available on the CPFT Intranet. Staff are also informed about the reporting of breaches / alerts / incidents via the CPFT induction process. Lessons learned from incidents will be fed back into future training or, where appropriate, to the staff concerned to encourage further participation and demonstrate the value of reporting to CPFT staff.

The Caldicott Guardian and SIRO are made aware of information governance related incidents / complaints / alerts reported and the associated action plans to mitigate similar incidents occurring in the future.

All staff will continue to be informed about the importance of reporting data security / information governance related incidents via a variety of communication methods such as staff bulletins, policies, procedures, specific training etc.

## **11. Monitoring and Review**

This process will be reviewed every two years, and in accordance with the following on an 'as and when required' basis:

- Legislative changes; good practice guidance; case law
- Significant incidents reported; new vulnerabilities
- Changes to organisational infrastructure.

## **12. Legislation and related documents**

A number of Trust policies are related to this procedure and all employees should be aware of this range below:

- Information Governance Policy
- Confidentiality and Access to Records & CCTV Policy
- Acceptable Use Policy (IT, Email, and Internet)
- Records Management Policy
- Information Risk Policy

- Incident Management Policy, including Serious Incidents & Near Misses

**Legal Acts:**

- Data Protection Act 2018
- UK General Data Protection Regulation
- Human Rights Act
- Freedom of Information Act 2000
- Thefts Act (1968 and 1978)
- Police and Criminal Evidence Act 1984 (PACE)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)

DRAFT

**Appendix A - Data Security / Confidentiality Audit (Observational on site )**

Audit completed by .....

Date .....

Observation detail	Response			Evidence / Findings /Action
	Yes	No	N/A	
<b>STAFF &amp; RESPONSIBILITIES</b>				
Staff member has evidence that they are compliant with their Annual Good Governance Mandatory Training <small>All staff must be compliant</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Staff member knows who the IG Manager and how to contact the IG Manager and the IG Team	<input type="checkbox"/>		<input type="checkbox"/>	
Staff member knows where to locate the Trust's Confidentiality, Information Security policies and procedures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Staff member is following the Standard Operating Procedure (SOP) when processing correspondence	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Observation detail	Response			Evidence / Findings /Action
	Yes	No	N/A	
Staff member is following the encryption guidance when sending out correspondence to non-secure email addresses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>ELECTRONIC SYSTEMS</b>				
Staff are observed to lock their screens using "control, Alt, Delete" when away from their desks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Staff are observed to remove their Smartcards when away from their desks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<b>MANUAL RECORDS &amp; PHYSICAL SECURITY</b>				
Manual records/patient/staff/business information are not left unattended on desks or unattended elsewhere in the office	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A confidential waste bin is in the office/ward near to the office for disposal of information no longer required	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>INCIDENTS &amp; NEAR-MISSES</b>				

Observation detail	Response			Evidence / Findings /Action
	Yes	No	N/A	
Staff know to and know how to report incidents and near-misses through appropriate channels as quickly as possible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Staff know to and how to report confidential breaches through appropriate channels as quickly as possible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

DRAFT

## **Appendix B – Privacy Officer Electronic Record Audit**

### **CPFT Privacy Office Role**

To ensure CPFT complies with the NHS Care Records Guarantee commitments, we are required to have Privacy Officers in place to investigate Access alerts/tasks generated by SystemOne, SystemOne Clinical Record Viewer (CRV) and Summary Care Record via (SCR).

The Trusts agreed process is that a random sample of SystemOne Privacy Alerts will be investigated on a monthly basis by the nominated Privacy Officers.

- ❖ A unit receiving less than 500 number alerts/warnings on a monthly basis will be required to investigate no less than 10% of the total received for the month.
- ❖ A unit receiving more than 500 number alerts/warnings on a monthly basis will be required to investigate no less than 5% of the total number received for the month.

All Clinical Record Viewer (CRV) Task Alerts and Summary Care Records (SCR) Alerts will be investigated.

The Privacy Officer (PO) role is delegated to nominated Clinical staff and Business Managers across the Trust.

The types of tasks and alerts generated by Patient Electronic Systems are:

#### **Clinical Record Viewer Task Alert Types:**

- Access Alert
- Create LR (self-claimed)
- Dissent Override
- Sensitive Data
- Stop Noted Record Access

#### **Summary Care Record Alert types:**

- Receive Self Claimed LR Alerts
- Receive Legal Override and Emergency View Alerts
- Receive Seal alerts
- Investigated via the TES Alert Viewer

#### **SystemOne Warnings & Alert Types:**

- Accessing records of deducted patients,
- Consent override
- Records with flagged errors
- Consent or dissent changed
- When a legitimate relationship has not been declared.

Appendix 1 below gives guidance for the nominated privacy officers to determine if access is appropriate and how to handle the task.

Appendix 2 gives guidance to all Privacy Officers on the Trust Process for investigating Alerts/Tasks.

Appendix 3 is the report template to be submitted to the Information Governance Manager on a monthly basis (1st working day month). Please send your monthly report to [informationgovernance@cpft.nhs.uk](mailto:informationgovernance@cpft.nhs.uk)

## SystemOne

### How to know if access is appropriate and how to handle tasks

Reason given for access	How to handle
Child re-presents in area	Check the re-present back to this area is there and the date of it make sense with the task date. If so, task can be marked completed. If not, ask the person who accessed the record to provide details, or query with the Team Manager.
Contact/query from family	Check it has been recorded. If so, task can be marked completed. If not, ask the person who accessed the record to provide details, or query with the service lead.
Complaint	Check with Service Lead; if they do not have the information, check with Pals if this matches the person accessing the record the task can be marked as completed, If not, ask the person who accessed the record to provide details, or query with the Team Manager.
Request for records	Check with Patient Information Service Team; and enter the records requests reference in the comments as the task is completed. This applies for any request, whether parents, police, or court order. Who requested the records must NOT be stated.
Safeguarding,	Check with the Lead Safeguarding Nurse if necessary.
Incident Investigation	Check with CPFT Patient Safety Team for name of Investigating Manager of Incident if this matches with person who has accessed the records task can be marked as complete if not ask the person who has accessed the records to provide details or, query with the Team Manager
Clinical supervision	Check Team Manager – (it should not normally be necessary to access deducted children’s records for supervision unless an incident is under investigation).
Research	Check consent to participation has been recorded (check with R&D Team)
CQC inspection / mock inspection	Enter inspector's name in comments box
Record correction	Check whether there is a mark in error entry that matches the date of the task and query with the Team Leader. This could happen when, for example, an item is scanned in error for another child’s record, and this is then discovered. The record still requires attaching to the correct child. (Records errors that are discovered only after child records have been deducted must be reported as IG incidents on DATIX)
Opened in error	Flag any concerns to Service Lead e.g. Child is/was/may be family member of person who accessed the record; child has been in the media, etc. Otherwise, check if this has happened more than once on this record - see S1 manual for how to do this. If it has, flag to service lead, otherwise put "human error" in comment box and mark as complete.

Caldicott	Head of Information Governance or Caldicott Guardian only. IG access to be checked with CG; check with IG that Caldicott access has been logged.
Audit	Only current records are audited for record keeping check with the Team Manager that the person accessing the record matches was auditing records, if they match mark the task as complete and close, if they do not match query with the Team Manager
ANY OTHER REASON	Check with Information Governance Manager

## Privacy Officer /Business Manager Process for Investigating Alerts & Warnings



