Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 5197

**Please reply to:**
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

11 January 2019

**Freedom of Information Act 2000**

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to Data security and cyber awareness.

You asked:

1. *Does the organisation have training that covers:*
a. *Recognising and reporting Phishing emails*
b. *Recognising Tailgating and how to respond (challenging strangers, checking for ID etc.)*
c. *Disposal of confidential information*
d. *Dangers of using USB sticks being given away or finding one that looks like it has been dropped*
2. *Does the organisation allow the use of USB sticks?*
3. *Does the organisation deliver specialised training to key staff (those staff that could be targeted as part of a phishing email campaign, i.e. finance, execs etc.)?*
4. *Does the organisation perform confidentiality audits as per the Data Security & Protection Toolkit?*
*Can you also answer relating to the audits:*
a. *Where the audits are undertaken would these be organised with the local team manager or the head of department i.e. the director etc.?*
b. *Would an audit ever be carried out unannounced?*
c. *Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy.*
d. *Do you record the results on a checklist / report and return the key contact? – if so can you supply a blank copy.*
5. *Does the organisation have confidential waste receptacles placed through the entire organisation and are they regularly emptied?*
6. *Does the organisations Exec board receive board level training relating to Cyber Awareness?*

7. *How does the organisation provide Data Security & Protection Training to staff, does the organisation use (please select all the options that are applicable):*

Trust response:

1.
a. Yes
b. Yes
c. Yes
d. Yes
2. Trust issued encrypted sticks only
3. Yes
4. Yes
a. Local Manager
b. Yes
c. Confidentiality Audit Procedure below. Please note this procedure is in draft form and is going through finalisation. Appendix 4 is currently in use by the Trust and is being incorporated into the policy.
d. See Confidentiality Audit Procedure
5. Yes
6. Yes
7.
a. ☐
b. ☐
c. Yes
d. Yes
e. ☐

**MAIDSTONE AND TUNBRIDGE WELLS NHS TRUST**

# Confidentiality Auditing and Monitoring of IT Systems Policy and Procedure

| | |
|---|---|
| **Target audience:** | Information Asset Owners and System Administrators |
| **Main author:** | Head of Information Governance<br>**Contact details: 01892 634029** |
| **Other contributors:** | Insert job title [optional] |
| **Executive lead:** | Chief Nurse/Senior Information Risk Owner |
| **Directorate:** | Health Informatics |
| **Specialty:** | Information Governance |

| | |
|---|---|
| **Supersedes:** | Not applicable |
| **Approved by:** | Information Governance Committee |
| **Ratified by:** | Policy Ratification Committee, DD MMMMMMM YYYY |
| **Review date:** | 2021 |

**Document history**

| | |
|---|---|
| **Requirement for document:** | • Data protection and security standard 4 |
| **Cross references (external):** | 1. National Data Guardian for Health and Care – Review of Data Security, Consent and Opt-Outs – June 2016<br>2. Your Data: Better Security, Better Choice, Better Care – July 2017 |
| **Associated documents (internal):** | • Information Governance Policy and Procedure - RWF-OPPCS-NC-TM9<br>• Information Security Policy and Procedure - RWF-OPPCS-NC-TM11 |

| | | | |
|---|---|---|---|
| **Keywords:** | **Audit** | **IT System** | **Confidentiality** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| **Version control:** | | |
|---|---|---|
| **Issue:** | **Description of changes:** | **Date:** |
| 1.0 | First iteration to assist the Trust in meetings its obligations under the Data Protection and Security Standard 4 | September 2018 |
| | | |

**Policy statement for**

# Confidentiality Auditing and Monitoring of IT Systems

This Confidentiality Auditing and Monitoring of IT System Policy and Procedure outlines the approach, methodology and responsibilities for auditing the confidentiality and safety of Maidstone and Tunbridge Well NHS Trust's information.

This document sets out the Trust's procedure for carrying out confidentiality audits across all departments. A purpose of the audit is to check that staff who have access to personal information have a legitimate authorised right to do so.

# Confidentiality Audit and Monitoring of IT Systems Procedure

*N.B. The table of contents below is designed to update using the headings that have been used in the Policy. Do not therefore amend the text in the Table of contents – just right-click the mouse and choose the "Update Field" option once the content of the document is finalised*


**Insert flow diagram of procedure to be followed [optional]**Error! Bookmark not defined.

**1.0 Introduction and scope** ..... **7**

**2.0 Definitions / glossary** ..... **7**

**3.0 Duties** ..... **7**

**4.0 Training / competency requirements** ..... **9**

**5.0 Procedure** ..... **9**

**APPENDIX 1** ..... **12**
**Process requirements** ..... **12**

**APPENDIX 2** ..... **13**
**CONSULTATION ON: Insert title of policy / procedural document** ..... **13**

**APPENDIX 3** ..... **13**
**Equality impact assessment** ..... **13**

**FURTHER APPENDICES** ..... **12**

## 1.0 Introduction and scope

Good practice requires that all organisations that handle personal and corporate sensitive information put in place control mechanisms to manage and safeguard confidentiality, including mechanisms for highlighting problems such as incidents, complaints and alerts.

The protocol provides and assurance mechanism by which the effectiveness of controls implemented within the Trust are audited, areas for improvement and concern highlighted and recommendations for improved control and management within the Trust are made.

Confidentiality audits will focus primarily on electronic records systems, the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of weak, non-existent or poorly applied controls.

Use of this protocol is to facilitate the detection and investigation of unauthorised and unacceptable access to records where individuals accessing records are not directly involved in a patient's care or matters associated with the employment of a staff member.

This protocol is relevant to all system managers, line managers and Information Asset Owners (IAOs) who have responsibility and accountability for the safe access of patient or staff personal and confidential information by Maidstone and Tunbridge Wells NHS Trust (the Trust) staff, or staff in the wider health and care economy who may access the Trust systems and records.

## 2.0 Definitions / glossary

Insert the definitions / explanation of key terms / acronyms that are used in the policy and procedural document here **[compulsory].**

## 3.0 Duties

### Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is accountable for information risk within Maidstone and Tunbridge Wells NHS Trust and advises the Board on the effectiveness of information risk management across the organisation. Operational responsibility for Information Security shall be delegated by the SIRO to the Trust Information Security Officer.

All Information Security risks shall be managed in accordance with the Trust Risk Management Policy.

The SIRO shall be responsible for ensuring the appointment of Information Asset Owners (IAO) to be responsible for Information Assets in their area(s) of responsibility.

**Head of Information Governance and Information Security Officer**
The Head of Information Governance and Information Security Officer is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes. The Head of Information Governance and Information Security Officer shall:

- Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for information security.
- Ensure the operational effectiveness of security controls and processes.
- Monitor and co-ordinate the operation of the Information Security Management System.
- Be accountable to the SIRO and other bodies for Information Security across Maidstone and Tunbridge Wells NHS Trust.
- Monitor potential and actual security breaches with appropriate expert security resource.

**Caldicott Guardian**
The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.

**Data Protection Officer**
The Data Protection Officer is responsible for ensuring that Maidstone and Tunbridge Wells NHS Trust and its constituent business areas remain compliant at all times with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer shall:

- Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.
- Provide a central point of contact for the Act both internally and with external stakeholders (including the Office of the Information Commissioner).
- Communicate and promote awareness of the Act across the Trust.
- Lead on matters concerning individuals right to access information held by the Trust and the transparency agenda.

**Information Asset Owners (IAOs)**
The IAOs are senior/responsible individuals involved in running the business area and shall be responsible for:

- Understanding what information is held.
- Knowing what is added and what is removed.
- Understanding how information is moved.

- Knowing who has access and why.
- Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks
- Supporting personal accountability of users within the business area(s) for Information Security
- Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries Trust policies and procedures.

**Information Asset Administrator/s (IAA)**

The IAAs have operational responsibility for managing access to Information Systems and Reports in line with agreed access guidelines.

**All Staff**

All professionals within health and social care and third parties working for or with the Trust are responsible for ensuring that, within their own practice they comply with the relevant professional standards as well as those standards defined locally and nationally.

## 4.0 Training / competency requirements

System managers are required to have the necessary competencies to completed these audits and monitoring activities are part of their ongoing day to day responsibilities.

Further advice and guidance is available from:

Head of Information Governance 07711 387964

## 5.0 Procedure

5.1. In order to provide assurance that access to personal information is gained only by those individuals that have a legitimate right of access, it is necessary to ensure that appropriate monitoring is undertaken either when a concern regarding inappropriate access is identified or by the means of periodic audits undertaken by Information Asset Owners and System Managers.

5.2. The Information Asset Owner is responsible for ensuring audits are completed in order that irregularities regarding access to confidential information can be identified, reported to the Information Governance Manager and action taken to address the situation. This will be either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

5.3. Actual or potential breaches of confidentiality should be reported to the Head of Information Governance (at least within 72 hours of the event) and an incident report submitted via Datix in order that action can be taken to prevent further breaches taking place. This also gives the Head of

Information Governance the opportunity to assess if the incident falls within the Serious Incident Requiring Investigation (SIRI) category. The Head of Information Governance is responsible for ensuring that the Information Governance Committee is informed of any concerns highlighted as a result of monitoring access to person identifiable information. Should unauthorised access to person identifiable information be highlighted by any individual, this will be dealt with in accordance with the Trust's disciplinary procedures.

5.4. Audit Process:

5.4.1 Information Asset Owners request the System Managers to undertake an audit, both technical and operational, at least annually to identify:

- Inappropriate access to a record without having a legitimate requirement to do so (including past employees/locums/contractors/third party staff);
- Repeated failed attempt to access information;
- Successful access to confidential information by unauthorised persons;
- Evidence of shared login sessions/passwords;
- Staff attempting to access their own or other family/friends information, safeguarding issues and patients who are considered to be very important persons (VIPs);

5.4.2 Reports will be shared with each of the Information Asset Owners/ Managers of the staff identified within the audit to investigate whether the access is legitimate and appropriate.

5.4.3 Findings of these internal investigations will be fed back to the Head of Information Governance for the inclusion in a report to the Trust Senior Information Risk Owner (SIRO)

5.4.4 Emergent concerns will be reported to the Trust Human Resources Department for further investigation and necessary action in line with Trust disciplinary procedures.

5.5 The confidentiality audits will be carried out at least annually, utilising the questionnaire in Appendix 4, on the Trust's key systems (as identified in Appendix 5) and periodically for all other systems

## 5.6 Implications of not following Access to Records procedures

Failure to ensure that patient and staff confidentiality is maintained may lead to:

- Disciplinary action up to and including gross misconduct against any member of staff failing to uphold the confidentiality of patient or staff records;
- Staff prosecution by the Information Commissioner's Office (ICO) under Section 55 of the Data Protection Act;

- Breaches of the Data Protection Act with the potential to be fined up to €20 million;
- Complaints from members of the public to the Trust or direct to the ICO;
- Damage to the Trust reputation;
- Care Quality Commission requirements not met with the potential for fines being imposed.

## Useful Contacts

Gail Spinks, Head of Information Governance, gspinks@nhs.net

Claire O'Brien, Chief Nurse/SIRO, clairem.obrien@nhs.net

Peter Maskell, Medical Director/Caldicott Guardian, Peter.Maskell@nhs.net

Kevin Rowan, Trust Secretary/Data Protection Officer, kevinrowan@nhs.net

## APPENDIX 1

## Process requirements

### 1.0 Implementation and awareness

- Once ratified the Policy Ratification Committee (PRC) Chair will email this policy/procedural document to the Clinical Governance Assistant (CGA) who will activate it on the Trust approved document management database on the intranet, under 'Policies & Q-Pulse'.
- A monthly publications table is produced by the CGA which is published on the Trust intranet under 'Policies & Q-Pulse'; notification of the posting is included on the intranet "News Feed" and in the Chief Executive's newsletter.
- On reading of the news feed notification all managers should ensure that their staff members are aware of the new publications.

### 2.0 Monitoring compliance with this document

- Implementation of this policy will be monitored by the Information Governance Committee via the standard item reviewing incidents and by audits undertaken by system managers.
- Breaches, if significant, may be reviewed by the Information Commissioner's Office.

### 3.0 Review

This policy and procedure and all its appendices will be reviewed at a minimum of once every 3 years, following the procedure set out in the 'Principles of Production, Approval and Implementation of Trust Wide Policies and Procedures' [RWF-OPPPCS-NC-CG25].

If, before the document reaches its review date, changes in legislation or practice occur which require extensive or potentially contentious amendments to be made, a full review, approval and ratification must be undertaken.

If minor amendments are required to the policy and procedure between reviews these do not require consultation and further approval and ratification. Minor amendments include changes to job titles, contact details, ward names etc.; they are 'non-contentious'. For a full explanation please see the 'Principles of Production, Approval and Implementation of Trust Wide Policies and Procedures' [RWF-OPPPCS-NC-CG25]. The amended document can be emailed to the CGA for activation on the Trust approved document management database on the intranet, under 'Policies & Q-Pulse'. Similarly, amendments to the appendices between reviews do not need to undergo consultation, approval and ratification.

### 4.0 Archiving

The Trust approved document management database on the intranet, under 'Policies & Q-Pulse', retains all superseded files in an archive directory in order to maintain document history.

**APPENDIX 2**

**CONSULTATION ON: Confidentiality Audit and Monitoring of IT Systems Policy and Procedure**

**Consultation process** – Use this form to ensure your consultation has been adequate for the purpose.

**Please return comments to:** Head of Information Governance – Gspinks@nhs.net

**By date:** 30/09/2018

| **Job title:** | **Date sent dd/mm/yy** | **Date reply received** | **Modification suggested? Y/N** | **Modification made? Y/N** |
|---|---|---|---|---|
| **The following staff MUST be included in ALL consultations:** | | | | |
| Clinical Governance Assistant ruthdickens@nhs.net | | | | |
| Staff-Side Chair debbie.oreiley@nhs.net | | | | |
| Emergency Planning Epo.mtw@nhs.net | | | | |
| Head of Staff Engagement and Equality jo.petch@nhs.net | | | | |
| Health Records Manager Louise.dunkley@nhs.net | | | | |
| Complaints & PALS Manager angelasavage@nhs.net | | | | |
| | | | | |
| All members of the approving committee: Information Governance Committee | | | | |
| The following staff have given consent for their personal names to be included in this policy and its appendices: | | | | |
| Ruth Dickens, Debbie O'Reiley, Jo Petch, Louise Dunkley, Angela Savage | | | | |
| The role of those staff being consulted upon as above is to ensure that they have shared the policy and procedure for comments with all staff within their sphere of responsibility who would be able to contribute to the development of the policy and procedure. | | | | |

**APPENDIX 3**

**Equality impact assessment**

This policy includes everyone protected by the Equality Act 2010. People who share protected characteristics will not receive less favourable treatment on the grounds of their age, disability, gender, gender identity, marital or civil partnership status, maternity or pregnancy status, race, religion or sexual orientation. The completion of the following table is therefore mandatory and should be undertaken as part of the policy development and approval process. **Please note that completion is mandatory for all policy and procedure development exercises.**

| | |
|---|---|
| **Title of policy or practice** | Confidentiality Auditing and Monitoring of IT Systems |
| **What are the aims of the policy or practice?** | To outline the approach, methodology and responsibilities for auditing the |

| | |
|---|---|
| | confidentiality and safety of Maidstone and Tunbridge Well NHS Trust's information. |
| **Is there any evidence that some groups are affected differently and what is/are the evidence sources?** | None |
| **Analyse and assess the likely impact on equality or potential discrimination with each of the following groups.** | Is there an adverse impact or potential discrimination.<br>No. |
| Gender identity | None |
| People of different ages | None |
| People of different ethnic groups | None |
| People of different religions and beliefs | None |
| People who do not speak English as a first language (but excluding Trust staff) | None |
| People who have a physical or mental disability or care for people with disabilities | None |
| People who are pregnant or on maternity leave | None |
| Sexual orientation (LGB) | None |
| Marriage and civil partnership | None |
| Gender reassignment | None |
| **If you identified potential discrimination is it minimal and justifiable and therefore does not require a stage 2 assessment?** | Not applicable. |
| **When will you monitor and review your EqIA?** | Alongside this policy/procedure when it is reviewed. |
| **Where do you plan to publish the results of your Equality Impact Assessment?** | As Appendix 3 of this policy/procedure on the Trust approved document management database on the intranet, under 'Trust policies, procedures and leaflets'. |

## FURTHER APPENDICES

The following appendices are published as related links to the main policy /procedure on the Trust approved document management database on the intranet, under 'Policies & Q-Pulse':

| No. | Title | Unique ID | Title and unique id of policy that the appendix is primarily linked to |
|---|---|---|---|
| 4 | Confidentiality Audit Questionnaire | | |

| No. | Title | Unique ID | Title and unique id of policy that the appendix is primarily linked to |
|---|---|---|---|
| 5 | Critical Systems List | FOI Exempt – Section 31 | |

**Appendix 4**

**Confidentiality Audit Questionnaire**

| | | |
|---|---|---|
| Are there any records or other personal data left unattended and not in use? | Yes | No |
| Is there any personal data sitting near window ledges or on show in public areas/reception areas e.g., on Whiteboards, PC screens, Etc. | Yes | No |
| Are there any posters and leaflets in the office/ward/department providing patients with details on how their information is or will be used? | Yes | No |
| Are there any USB Sticks or other removable media i.e., CDs, DVDs used within the office/ward/department | Yes | No |
| If yes what removable media is used and how many? | | |
| | | |
| If yes, are they stored securely? | | |
| | | |
| If yes, where are they stored and are they encrypted? | | |
| | | |
| Are there any USB stock or other removable media left unattended? | Yes | No |
| Do staff use mobile working devices? | Yes | No |
| If yes, have staff been made aware of the guidelines around this? | Yes | No |
| How are the guidelines communicated to staff? | | |
| | | |
| Are there any Dictaphones or digital cameras used within the office/ward/department? | Yes | No |
| If yes, what devices are used and how many? | | |
| | | |
| If yes, are they stored securely? | | |
| | | |
| If yes, are they encrypted? | | |
| | | |
| Are there any Dictaphones or digital cameras left unattended | Yes | No |
| Are any records stored in a storage area | Yes | No |
| If yes, is the storage area or cabinet locked with a key or code | Yes | No |
| Are they keys/code easily accessible to people | Yes | No |
| Are records archived and disposed f in line with the Trust's records management policy? | Yes | No |
| Is there a fax machine within the office/ward/department | Yes | No |
| If yes, is the fax machine in a safe haven place i.e., it is not sited next to a public area, a reception area or window ledge | Yes | No |

| | | |
|---|---|---|
| Are fax numbers programmed into the fax machine | Yes | No |
| Are any faxes left unattended? | Yes | No |
| | | |
| Are there any unattended PCs left unlocked for people to view or access | Yes | No |
| If yes, what information/systems are visible on screen | | |
| | | |
| Are screens visible from doors or windows | Yes | No |
| Are windows and/or doors covered by blinds or curtains | Yes | No |
| Are any of the PCs in public areas | Yes | No |
| Does the office/ward/department have any laptops, IPads or other tablet devices | Yes | No |
| If yes, what devices are held and how many | | |
| | | |
| Are they stored securely and are they encrypted | | |
| | | |
| **System Specific** | | |
| | | |
| Is this the latest available version of the system software? | Yes | No |
| If this is **not** the latest available version of the system software are there any adverse impacts for the Trust? | Please advise | |
| | | |
| What operating system interdependencies does the software have? | Please advise | |
| | | |
| Are the latest versions of the interdependent software installed? | Yes | No |
| Will upgrades be required in the next 12 months? | Yes | No |
| If yes, please detail | | |
| Has the system user database been checked against the latest employees list? | Yes | No |
| Is there a local procedure for checking that access granted to agency, local, contractor, third party employees is still valid? | Yes | No |
| If yes, please detail | | |
| Is system access to the network protected by passwords and logins? | Yes | No |
| Is the equipment security marked? | Yes | No |
| Is the equipment secure from theft i.e., IT devices are not left lying around | Yes | No |
| Does the office/ward/department save information to the network folders or to other storage i.e., C Drive or USB | Please advise | |
| | | |
| System manager is notified of leavers | Yes | No |
| System manager is notified of staff members change of role | Yes | No |
| No. of failed login attempts with a valid User ID (password guessing attempts | | |
| No. of failed login attempts with an invalid User ID | | |
| Failed password change attempts | | |

| | | |
|---|---|---|
| Has any evidence been found of shared login sessions/passwords | Yes | No |
| If yes, what action has been taken? | | |
| Successful attempts to access information without justification | | |
| Backups log files are maintained according to procedure | Yes | No |
| System clock is synchronised | Yes | No |
| VIP or high-profile patient record access is monitored | Yes | No |
| If yes, has any inappropriate activity been identified? | Yes | No |
| Users accessing records of family members Same Last Name checks completed | Yes | No |
| If yes, has any inappropriate activity been identified? | Yes | No |