Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 5868

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

07 January 2020

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 Bring Your Own Devices to Work.

You asked:

1. Does Maidstone and Tunbridge Wells NHS Trust allow staff to use their own devices to access work email? Please answer Yes or No.
2. Does Maidstone and Tunbridge Wells NHS Trust allow staff to use their own devices for any other work-related activities? Please answer Yes or No.
3. If you answered yes to question 2 please provide a list of the types of systems that staff can access from personally owned devices?
4. Does Maidstone and Tunbridge Wells NHS Trust have a policy that covers BYOD or the use of personal devices at work? Please answer Yes or No.
5. If you answered yes to question 4 please could you provide a copy of your policy that covers BYOD or personal device usage at work?

Trust response:

1. Yes
2. No
3. Not applicable
4. Yes
5. Please see the following policy.

MAIDSTONE AND TUNBRIDGE WELLS NHS TRUST

Information Security – Operational Security Policy and Procedure

Target audience:	All Trust staff
Main author:	Head of Information Governance **Contact details: 07711 387964**
Other contributors:	Based on template documents provided by NHS Digital
Executive lead:	Chief Nurse
Directorate:	Health Informatics
Specialty:	Information Governance
Approved by:	Information Governance Committee, 10 July 2019
Ratified by:	Policy Ratification Committee, 31 July 2019
Review date:	November 2023

Document history

Requirement for document:	• external recommendation of NHS Digital
Cross references (external):	1. Caldicott Data Guardian Principles 2. Data Protection Act 2018 3. Equality Act 2010 4. EU Waste Electrical and Electronic Equipment (WEEE) Directive 5. General Data Protection Regulation 2018 6. Government Security Classification Scheme (GSCS) 7. HMG mandatory requirements – Secure Sanitisation. 8. HMG Security Policy Framework – Security Policy No. 4 9. National Data Guardian's 10 Data Security Standards 10. UK Waste Electrical and Electronic Equipment Regulations 2006
Associated documents (internal):	• Business Continuity Plan [RWF-OPPM-CORP192] • Forensic Readiness Policy and Procedure • Incident Management Policy and Procedure [RWF-OPPPCS-NC-CG22] • Information Security Policy and Procedure [RWF-OPPCS-NC-TM11] • Information Security – Technical Security Policy and Procedure • ICT Acceptable Use Policy and Procedure [RWF-OPPCS-NC-TM8] • Management of White Boards • Resilience Policy and Procedure [RWF-OPPCS-NC-TM25] • Security Policy and Procedure [RWF-OPPPCS-NC-FH2] • Social Media Policy and Procedure [RWF-OPPCS-NC-TM38]

Keywords:	**Acceptable Use**	**Bring Your Own Device**	**Business Continuity**
	Clear Desk and Screen	**Data Handling**	**Disaster Recovery**
	Information Security	**Mobile and remote working**	**Password**
	Remote and	**Removable Media**	**Safe Haven**

	Mobile Working		
	Sanitisation, Disposal and Destruction	**Security Classification**	**Social Media**

Version control:		
Issue:	**Description of changes:**	**Date:**
1.0	First iteration of policy	March 2019

Summary for

Information Security – Operational Security Policy and Procedure

This Information Security – Operational Security Policy and Procedure is one of three supporting policies to the Information Security Policy which outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Maidstone and Tunbridge Well NHS Trust's information.

The Operation Security Policy and Procedure details how the security requirements are to be achieved for matters such as: data handling, mobile and remote working, disaster recovery and use of social media.

Information Security – Operational Security Policy and Procedure

1.0 Introduction and scope

The Trust Information Security – Operational Security Policy and Procedure should be read in conjunction with the Trust Information Security Policy and Procedure which outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Maidstone and Tunbridge Wells NHS Trust's information and is the overarching policy for information security.

This Information Security – Operational Security Policy and Procedure details how the security requirements are to be achieved for matters such as: Bring Your Own Device, Clear Desk and Clear Screen, Password Management, and Social Media as well as many other elements of operational security.

Terminology

Term	***Meaning/Application***
Shall	*This term is used to state a Mandatory requirement of this policy*
Should	*This term is used to state a Recommended requirement of this policy*
May	*This term is used to state an Optional requirement*

This policy applies to all Trust staff, students, and all volunteers and persons working under the terms of a contract. Where services are provided by external contractors, sub-contractors, agencies, temporary workers or third parties on the basis of a specification set by the Trust, these parties are responsible for adhering to the Trust's Policies and Procedures whilst providing services on behalf of the Trust.

2.0 Definitions / glossary

Term	**Definition**
Access	The permissions that are granted to a user, or to an application, to read, write and erase files in a computer. Access rights can be tied to particular folders or to specific programmes and data files.
Authentication	The process or action of proving or showing something to be true, genuine or valid.
Authorisation	Official permission or approval.
Backup	A copy of a file or other item or data made in case the original is lost or damaged.
Bullying	offensive, intimidating, malicious or insulting behaviour, or abuse or misuse of power through means intended to undermine, humiliate, denigrate or injure the recipient.
Business Continuity	The capability of an organisation to continue delivery or products or services at acceptable predefined levels

Term	Definition
	following a disruptive incident.
Bring Your Own Device (BYOD)	The practice of allowing employees to use their own computers, smartphones, or other devices for work purposes.
Compact Disc (CD)	A portable storage medium that can be used to record, store and play back audit, video and other data in digital form.
Data	The collection of characters or symbols on which operations are performed by a computer
Data Destruction	The process of destroying Data stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorised purposes.
Data Handling	The collecting, representing and analysing data .
Data Recovery	The process of retrieving inaccessible, lost, corrupted, damaged or formatted data from secondary storage, removable media or files..
Destruction	The action or process of causing so much damage to something that it no longer exists or cannot be repaired.
Device	A thing made or adapted for a particular purpose, especially a piece of mechanical or electronic equipment.
Disaster Recovery (DR)	An area of security planning that aims to protect an organisation from the effects of significant negative events. DR allows an organisation to maintain or quickly resume mission-critical functions following a disaster.
Discrimination	The unjust or prejudicial treatment of different categories of people as set out in the Equality Act 2010.
Discriminatory	Making or showing an unfair or prejudicial distinction between different categories of people or things.
Disposal	The action or process of getting rid of something.
DVD	A type of compact disc able to store large amounts of data, especially high-resolution audio-visual.
Electronic Media	Broadcast or storage media that take advantage of electronic technology. They may include television, radio, internet, fax, CD, DVD and any other medium that required electricity or digital encoding of information.
Email	Messages distributed by electronic means from one computer user to one or more recipients via a network.
Encryption	The process of converting information or data into a code,

Term	Definition
	especially to prevent unauthorised access.
Enterprise	A business or company or a project or undertaking.
Forensic Readiness	The ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation.
Government Security Classification Policy (GSCP)	Governance policy describing how information assets are classified to ensure they receive appropriate protection. All information is classified into three types: OFFICIAL, SECRET and TOP SECRET. Policy came into effect on 2 April 2014.
Harassment	Aggressive pressure or intimidation
Hardware	The machines, wiring and other physical components of a computer or other electronic systems.
HMG	Her Majesty's Government (the Government of the United Kingdom).
Impersonation	An act of pretending to be another person for the purpose of entertainment or fraud.
Information	Facts about a situation, person or event.
Information Asset Owner (IAO)	A senior member of staff who is the nominated owner for one or more identified information assets with the Trust.
Information Media	Media that disseminates printed or digital matter.
Information Security Officer (ISO)	Responsible for establishing and maintaining the enterprise vision, strategy and programme to ensure information assets and technologies are adequately protected. In this Trust the role is the by the Head of Information Governance.
Internet	A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communications protocols.
Intimidate	To frighten or overawe someone, especially in order to make them do what one wants.
Intimidation	The act of intimidating someone, or the state of being intimidated
IT Systems	A system composed of computers and software used to run a computerised databases.
Laptop	A computer that is portable and suitable for use while travelling.
Log-off	Go through the procedures to conclude use of a computer, database or system.

Term	Definition
Mobile Device Management	The administration, usually with a third party product, of mobile devices such as smartphones, tablet computers and laptops.
Password	A string of characters that allows access to a computer, interface or system.
Patches	Software designed to update a computer programme or its supporting data, to fix or improve it.
Physical Security	The protection of personnel, hardware, software, networks and data from physical actions and events that would cause serious loss or damage.
Pornographic	Constituting or resembling pornography.
Pornography	Printed or visual material containing the explicit description or display of sexual organs or activity, intended to stimulate sexual excitement.
Publish	To prepare, issue, communicate information to a third party.
Remote Wipe	A security feature that allows a network administrator or device owner to send a command to a computing device and delete data.
Reuse	Use again or more than once.
Removable Media	Any type of data storage device that can be removed from a computer while the system is running. Examples include CDs, DVDs as well as diskettes and USB drives.
Safe Haven	A location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.
Secure Sanitisation	The process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable.
Security Classification	Used to indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse).
Senior Information Risk Owner (SIRO)	The Board level member of staff accountable for information risk within Maidstone and Tunbridge Wells NHS Trust and who advises the Board on the effectiveness of information risk management across the organisation. In this Trust the role is held by the Chief Nurse.
Sensitive information	Data that must be protected from unauthorised access to safeguard the privacy or security of an individual or

Term	Definition
	organisation
Single Points of Failure	A part of a system that, if it fails, will stop the entire system from working.
Social Media	Websites and applications that enable users to create and share content or to participate in social networking.
Social Networking	The use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own.
Universal Serial Bus (USB) Stick	A small external piece of equipment that can be connected to a computer or other piece of electronic equipment to copy and store information.
Violent	Using or involving physical force intended to hurt, damage or kill something or someone.
WhiteBoard	A board with a smooth, white surface, often attached to a wall, on which you can write and draw using special pens

3.0 Duties

Person/Group	Duties
Caldicott Guardian	The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data. In this Trust the post is held by the Medial Director.
Data Protection Officer (DPO)	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 legislation. 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. In this Trust the role is held by the Trust Secretary.

Person/Group	Duties
Information Asset Owners (IAOs)	The Information Asset Owners (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 of this policy and associated policies and procedures.
Information Security Officer (ISO)	Responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes. The 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. In this Trust the post is held by the Head of Information Governance.

Person/Group	Duties
Senior Information Risk Owner (SIRO)	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. In this Trust the post is held by the Chief Nurse.
All Staff	Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Trust business. All staff are responsible for information security and remain accountable for their actions in relation to NHS and other UK Government information and information systems. Staff shall ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

4.0 Training / competency requirements

4.1 General

No specific training/competency requirements at this time other than completion of the mandatory annual Information Governance training. However, advice and guidance is available from:

Head of Information Governance	GSpinks@nhs.net
Head of Information Technology	Darren.twort@nhs.net
Local Security Management Specialist	Joanne.hand@nhs.net

4.2 Business Continuity

- Personnel who are required to undertake specific technical and functional roles associated with business continuity shall be trained and formally qualified to complete this specialist function.
- All Trust staff, including third parties, shall be made aware of the requirements of the Trust Business Continuity Plan and subsequent Procedures.

4.3 Disaster recovery

- Personnel who are required to undertake specific technical and functional roles associated with disaster recovery shall be trained and formally qualified to complete this specialist function.
- All Trust staff, including third parties, shall be made aware of the requirements of the Trust Disaster Recovery Plan and its Procedures.

5.0 Procedure

5.1 Acceptable Use

Information relating to the use of information systems can be found in the ICT Acceptable Use Policy and Procedure.

5.2 Security Classification

On 2 April 2014 the Government changed the way the UK classifies and marks its information. The new approach is called the Government Security Classification Scheme (GSCS).

This involves new ways of working with information below SECRET level. All such information is now to be classified OFFICIAL. The key change is that individuals are expected to take more personal responsibility for thinking about the security of the information they handle.

Maidstone and Tunbridge Wells NHS Trust shall comply with the GSCS.

5.2.1 *Three levels of security classification*

These are:

- **OFFICIAL**. The majority of information that is created or processed by Maidstone and Tunbridge Wells NHS Trust shall be security classified as **OFFICIAL**. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or disclosed inappropriately.
- A limited subset of **OFFICIAL** information could have more damaging consequences (for individuals, the NHS or the government generally) if it were lost, stolen or published in the media. Where information is identified as such, it shall still be managed within the **OFFICIAL** classification tier, but shall attract additional measures (generally procedural or personnel) to reinforce the 'Need to Know' (NTK). In such cases where there is a clear and justifiable requirement to reinforce the NTK, assets shall be conspicuously marked **OFFICIAL – SENSITIVE**.
- **SECRET**. Very sensitive information that justifies heightened protective measures to defend against a higher level of threat shall be marked as **SECRET**. For example, where compromise could lead to the disruption or loss of emergency and heath care capabilities, loss of public trust in the NHS or significant loss of reputation to the NHS with significant coverage by the national and international press. There is a significant step up between **OFFICIAL** and **SECRET**.

- **TOP SECRET.** The government's most sensitive information requiring the highest levels of protection from the most serious threats shall be marked as **TOP SECRET**. For example, where compromise could lead to the complete breakdown of trust by the public in the NHS, a complete loss of emergency and health care capabilities and total loss of reputation in the NHS with widespread condemnation by both the national and international press, or requiring a major government intervention and/or a public inquiry.

Access to sensitive information MUST only be granted on the basis of a genuine 'need to know' and an appropriate personnel security control.

5.2.2 *Descriptors*

Some information (including electronic documents) may carry further security markings along with the classification to indicate the sensitivity of the information they contain. The rules for applying these security markings apply to all information, in both paper and electronic form. These markings are known as 'Descriptors' and indicate why the information is sensitive.

Maidstone and Tunbridge Wells NHS Trust shall only use descriptors in conjunction with a security classification and in the main will be used with the **OFFICIAL – SENSITIVE** marking. It is not envisaged that they will be used with **SECRET** and **TOP SECRET** because all information at these classifications must be handled and shared to ensure it is only accessed by those who need to know it.

Descriptors should only be used in the following circumstances:

- **COMMERCIAL** – To identify commercial or market-sensitive information, including that which is subject to statutory or regulatory obligations that

may be damaging to the Trust, the wider NHS or government or to a commercial partner if improperly accessed.

- **PERSONAL** – To identify Personal Data (as defined by the Data Protection Act) whose release or loss could cause harm, distress or detriment to the individual(s) to whom it relates. Maidstone and Tunbridge Wells NHS Trust must ensure that it fulfils its obligations under the Data Protection Act.
- **LOCSEN** – To identify sensitive information that refers to the department or organisation in which it was produced.

5.2.3 *Mapping to Previous Protective Marking Scheme*

- There is no requirement for the Trust to retrospectively reclassify or remark existing information, data or systems with the new security classification markings.
- For information bearing the 'old' markings, the Trust shall follow the guidance below to ensure appropriate handling.
- Unless there are specific instructions to the contrary, Trust staff shall maintain current levels of control and use existing IT systems on which information is currently held/processed.

The table below provides a mapping that the Trust can use to ensure that it correctly handles information bearing the old markings or information bearing no marking at all.

Old Marking	New Classification	Examples
UNCLASSIFIED/ NOT PROTECTIVELY MARKED	Treat as **OFFICIAL** (unmarked) Where controls prevent otherwise safe sharing of non-sensitive information IAOs have some discretion to relax controls, provided any relaxations are specific to their assets and have no wider risk consequences (e.g. for the security of IT assets and GSI/PSN code of connection).	▪ Public notices and leaflets ▪ Published information ▪ Information that doesn't contain personal data or other sensitive content ▪ Training materials
PROTECT (Including NHS PROTECT)	If information relates to general administration, treat as **OFFICIAL** (unmarked). Where used for personal data, maintain existing handling controls. Unless a risk assessment has identified the requirement for additional security controls personal data will be treated as **OFFICIAL**. Information assessed as containing particularly sensitive content will need to be marked	▪ Documents containing personal data i.e. personnel records ▪ General administration not intended for publication

	OFFICIAL – SENSITIVE, though these instances may already have been marked **RESTRICTED** or **CONFIDENTIAL**.	
RESTRICTED	If it relates to general administration there should be a presumption that it can be treated as **OFFICIAL** (unmarked).	▪ General administration ▪ Policy documents ▪ Commercial documents
	Where used for personal data, maintain existing handling controls. Unless a risk assessment has identified the requirement for additional security controls data will be treated as **OFFICIAL.** Information assessed as containing particularly sensitive content will need to be marked **OFFICIAL – SENSITIVE**, though these instances may already have been marked **RESTRICTED** or **CONFIDENTIAL**. It needs to be considered whether the subject matter is particularly sensitive and there is a need to restrict access, in which case material may additionally require handling/marking as '**OFFICIAL – SENSITIVE**'. Anything with this level of sensitivity may already have agreed handling constraints. If there is any doubt, it should be discussed with the Information Asset Owner (IAO).	▪ The majority of documents containing personal data i.e. personnel records ▪ Commercial information and contracts ▪ Management information, strategy and organisational proposals
CONFIDENTIAL (Including NHS CONFIDENTIAL)	Treat as **OFFICIAL – SENSITIVE** unless there is a clear national security aspect in which case treat as **SECRET**. If there is a need to reproduce content, check the security classification with the author/originator or IAO.	▪ Material relating to system designs and implementation ▪ Material relating to security incidents and security risks ▪ Material relating to medical and health records ▪ Material relating to criminal investigations ▪ Material relating to disciplinary matters
SECRET	Continue to treat as **SECRET**.	It is likely that only a

	(Seek further advice from the Head of Information Governance or asset IAO).	very small amount of material (if any) will fall into this category
TOP SECRET	Continue to treat as **TOP SECRET**. (Seek further advice from the Head of Information Governance or asset IAO).	It is likely that only an extremely small amount of material (if any) will fall into this category

Further information is available from https://www.gov.uk/government/publications/government-security-classifications

5.3 Clear Desk and Screen

5.3.1 Clear Desk

Reasonable steps shall be taken at the end of the working day or when leaving the office during the day to secure documents in a lockable office or in lockable furniture (desk drawers, filing cabinets, cupboards).

If an office remains occupied for the duration of your absence information at OFFICIAL – SENSITIVE or NHS Confidential may be left on the desk provided those present are authorised to view the information, otherwise it should be removed from view or secured appropriately.

If material at OFFICIAL – SENSITIVE or NHS Confidential has been left unsecured, you shall either stay with it until the data owner returns or secure the material before you leave.

Information classified as SECRET shall not be left unattended for any period of time. When not in use, it is to be secured in a cabinet approved to store SECRET assets.

Removable media shall be locked away.

Personal belongings should be removed from view.

Office/work area windows shall be closed when working areas are unattended and at the end of the working day and blinds, if fitted, should be drawn.

All internal doors shall be closed when working areas are unattended and at the end of the working day.

In ground floor work areas, blinds shall be closed so PC/Laptop screens, information boards or any protectively marked or sensitive information cannot be viewed by passers-by.

All desk pedestals shall be locked when working areas are unattended and at the end of the working day.

All cabinets shall be locked when working areas are unattended and at the end of the working day.

All printers shall be cleared of printed material when working areas are unattended and at the end of the working day.

All photocopiers shall be cleared of printed material when working areas are unattended and at the end of the working day.

All ‘white boards’ shall be managed in line with Appendix 4 to this policy.

All ‘flip charts’ holding information at OFFICIAL – SENSITIVE or NHS Confidential information shall be secured when working areas are unattended and at the end of the working day.

5.3.2 Clear Screen

For all Maidstone and Tunbridge Wells NHS Trust IT systems, computer screens should be angled away from the view of unauthorised persons.

All users shall ensure that any information at OFFICIAL – SENSITIVE or NHS CONFIDENTIAL shall not be overseen by those without a need to know.

Screens shall be cleared or locked when talking to unauthorised persons.

By default all computer terminals shall have the auto screen saver set to activate when there is no activity for a period of no longer than 15 minutes inactivity. Computer terminals in clinical areas may have the period of inactivity extended to no longer than 30 minutes inactivity. (If users have access to SECRET material then the auto screen saver period shall be set for a period of no longer than 5 minutes inactivity). By exception the period of inactivity may be extended for clinical or business reasons – application to be made via the Head of Information Governance.

Users shall invoke the screen lockout for periods when they are away from their device for no longer than 45 minutes. For periods longer than 45 minutes and at the end of the working day they shall log-off or shut down the device and switch off the screen.

For IT systems processing SECRET information the screen lockout shall be invoked for a period of no longer than 30 minutes inactivity.

Users shall be required to re-authenticate to unlock their screens.

A list of devices authorised to stay 'on and accessible' throughout the working day is maintained by the IT department.

5.4 Data Handling

5.4.1 General

When handling data, all users shall do so in accordance with and be responsible for adherence to the Information Security – Operational Security Policy and the Trust Information Security – Security Management Policy. Periodic auditing of adherence to this policy shall be the responsibility of the Trust Head of Information Governance.

Users shall ensure that information is appropriately marked in accordance with Government Security Classification Scheme (GSCS) and any bespoke requirements as required by the wider NHS.

An approved level of protection shall be used in the transfer of data in relation to its level of security classification and privacy requirement.

Users shall ensure data is transferred only to named individuals and those who need to know and that data shall be kept to the minimum required.

Any mishandling of data in transfer or at rest shall be reported as an incident.

Users shall have authority (in writing) from the Information Asset Owner (IAO) to undertake the transfer.

A Data Access Agreement (DAA) or Data Sharing Agreement (DSA) should be produced, agreed and signed by all parties prior to any NHS data

containing Personally Identifiable Information (PII) or OFFICIAL-SENSITIVE data/information being passed or shared with any non-government or non-public authority body.

The Head of Information Governance or Head of IT should be approached for guidance and assistance where there is difficulty identifying a suitable method of transfer.

5.4.2 Safe Havens

The term ‘Safe Haven’ is used within the NHS to denote either a secure physical location or the agreed set of administrative arrangements that are in place to ensure security classified, personal or other sensitive information is communicated safely and securely.

Safe Havens should be established, where:

- Information can be securely received and transferred.
- Paper-based information is stored securely in approved containers, as soon as practical.
- IT is not on view or accessible to unauthorised persons.
- All waste potentially containing security classified, personal or other sensitive information is securely retained until it can be securely disposed of or destroyed.
- Conversations discussing security classified, personal or other sensitive information can be held where they cannot be overhead by unauthorised persons.

5.4.3 Digital/Internet Data Transfers

In addition to the general principles above, digital transfers shall adhere to the following:

- Only approved transfer methods shall be used and in accordance with the Security Classification of data.
- Data up to and including OFFICIAL – SENSITIVE may be sent within the PSN and the N3/HSCN without a need for encryption.
- An approved method of encryption shall be used for the transfer of OFFICIAL – SENSITIVE data that is sent outside the secure network.
- An approved method of encryption should be used for the transfer of OFFICIAL data that is sent outside the secure network.

5.4.4 Physical Data Transfers

Physical transfers include paper and portable physical media (USB, hard disks, CDs, DVDs, etc.) In addition to the general principles above at 5.4.1, physical transfers shall adhere to the following:

- A Trust management approved method of transfer shall be determined for the type of data being transferred.
- A record of custody of transfers shall be kept.
- All data (with the exception of hard copy transfers) shall be stored encrypted (using a Trust approved method) for transfer regardless of classification.
- An approved method of transfer shall be determined for the type of data being transferred.
- Portable media shall only be authorised when there is a valid business requirement.
- Only official Trust approved removable media shall be used.
- Where information is transferred via mail the outer envelope/package shall not be marked with its Security Classification.

Transfers of data in hard copy form will need to be protected, by using such methods as approved couriers or Royal Mail Track and Trace. Where data is to be transferred by memory stick, CD/DVD or removable hard drive, the media should be encrypted, which will provide adequate protection should it become lost or fall in to the hands of unauthorised persons.

5.4.5 Data Disposal

Information held on ICT systems **shall** be securely erased in accordance with HMG mandated requirements and the Trust Information Security – Operation Security Policy Section 5.8 Sanitisation, Reuse, Disposal and Destruction.

Information held in paper form **shall** be securely destroyed in accordance with the NHS Records Management Policy.

5.4.6 Other Data Handling

Where there are occasions when new pieces of work require one time only data transfers or data storage, Trust staff **should** request guidance from the Head of Information Governance or Head of IT.

5.5 Mobile and Remote Working

The benefits of mobile and remote working are considerable. The Trust must ensure that business can be conducted remotely with the confidence that sensitive information remains protected and secure. Mobile and remote users must be fully aware of and compliant with the relevant policies and legislation. More information relating to the use of mobile and remote working can be found in the ICT Acceptable Use Policy and Procedure.

5.6 Password Management

5.6.1 General

Passwords shall be used to ensure that access to NHS systems, devices and information is controlled and restricted to approved and authorised users only.

Passwords shall be enforced and used on systems and devices under the control of Maidstone and Tunbridge Wells NHS Trust.

Passwords shall be complex in nature and follow HMG guidance and best practice.

5.6.2 Password Creation

Unique passwords shall be created, and used by individuals for each system to which they require access (these will be created under the direction of the relevant system administrators as systems may have differing requirements).

As a best practice guide, passwords should be created in the following format:

- A minimum of 8 characters long.
- Not contain a dictionary word of more than 4 characters.
- Contain at least two uppercase letters.
- Contain at least two lower case letters.
- Contain at least 2 numbers.
- Contain at least two special characters or non-alphanumeric characters, such as ! ” £ $ % & * @.

5.6.3 Password Security

All passwords shall be protected to the same level as that afforded to the system or information that they provide access to.

Users shall ensure that if passwords are to be written down they shall be stored in a personal lockable storage device.

Users shall ensure that passwords are not shared with other users.

Users shall ensure that passwords are never revealed to any other persons. This includes system administrators, security staff and management.

All Local Server Administrator passwords should be changed every 90 days.

If there is any indication that a password has been compromised that password shall be changed immediately and reported as a security incident.

The Local Administrator Account passwords shall differ from domain administration.

Separate login and passwords shall be required for administrators to undertake normal day to user functions.

No passwords shall be incorporated in the hard coding of user accounts in application code.

5.6.4 Password Management

Systems shall be configured to ensure that passwords meet the required criteria (length, complexity, etc.) for that particular system.

All new or reset passwords shall be changed immediately upon 1st log on.

Systems should be configured to force the change of passwords at regular intervals. These intervals should be of sufficient frequency to aid security, but not too frequent that this causes problems for users and administrators.

Systems shall be configured to ensure that passwords, if stored, are held in a secure format (i.e. encrypted).

Systems shall be configured to ensure that previously used passwords cannot be reused within the next 3 resets.

Systems shall be configured to ensure that following the incorrect entering of a password a specified number of times, the account is locked and can only be opened/reset through a system administrator process. This specified number needs to be small enough in order to add a level of security to the system, but not too small that it causes a burden for user and administrator alike.

Users shall ensure that different passwords are allocated and used on different systems (separate passwords for email account and network logons).

Users shall ensure one password is not simply a derivative of another.

5.7 Removable Media

5.7.1 General

- By default, all desktops under the control of the Trust shall have USB ports disabled and read access only via DVD drive. Any requirement to deviate from this shall require formal authorisation and business justification with line manager approval prior to submission to the Head of Information Governance.
- The use of removable media shall only be authorised when there is a valid business requirement.
- Only official Maidstone and Tunbridge Wells NHS Trust approved removable media shall be used.
- Where removable media is allowed to be used it shall be scanned with an approved anti-virus product prior to use.
- Where there is a requirement for data to be burned to CD/DVD or copied to other removable media, this shall have approval of the relevant Information Asset Owner (IAO) for the data.
- The IAO shall consider if there is a requirement to encrypt the data to an appropriate standard prior to burning to CD/DVD or copying to other removable media. Where the data is personal confidential then encryption must be utilised.

5.7.2 Removable Media Classification

- Hardware containing media shall be classified at the security classification of the information contained on the media.
- Non-volatile media shall be classified to the highest security classification of information stored on it.
- Removable media shall be reclassified if information copied onto that media is of a higher security classification or is subject to a security classification upgrade.

5.7.3 Removable Media Labelling

- All removable media shall be physically labelled with a marking that states the maximum security classification of the data held.
- Security classification markings on removable media shall be easily visually identifiable.

5.7.4 Removable Media Handling

- All users shall comply with the Trust Data Handling procedure outlined in section 5.3 and the Security Policy, when handling removable media that:
- Holds or has held security classified or sensitive data or information
- Is or has been connected to systems that hold or have held classified or sensitive information.

5.7.5 Removable Media Sanitisation

- The Trust shall document procedures for the sanitisation of media, which are regularly tested.
- The Trust shall ensure all media types which contain information are dealt with in accordance with the latest HMG mandatory requirements for Secure Sanitisation.

5.7.6 Removable Media Destruction & Disposal

- The procedures for secure disposal of media containing confidential information shall be proportional to the sensitivity of that information.
- Removable Media shall be disposed of when no longer required, in accordance with the latest HMG mandatory requirements for destruction and disposal.
- When accumulating media for disposal, consideration should be given to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

5.8 Sanitisation, Reuse, Disposal and Destruction of Electronic Media

5.8.1 General

- The Sanitisation, Reuse, Disposal and Destruction Policy shall be used to enable appropriate and authorised sanitisation, reuse or destruction methods to be deployed when re-using or disposing of electronic media to ensure that that the data cannot be reconstructed, recovered or

retrieved and made available to persons who do not have a ‘need to know’ or should not have access to the data.

5.8.2 Sanitisation, Disposal and Destruction Methodologies

- The type of sanitisation, disposal and destruction methods deployed shall be based on:
  - The impact to the Trust (and the wider NHS) if the confidentiality of the data is breached
  - The type of electronic storage media
  - Whether the media is to be re-used and if so, where the electronic media will be re-used.
- The sanitisation and destruction method used shall be in accordance with the latest HMG mandatory requirements for Secure Sanitisation (which can be found via the NCSC website).

5.8.3 Encryption

- Encryption is not a sanitisation method and the Trust shall ensure that it is not relied on as a means of securing data when disposing of electronic media for re-use. When disposing of encrypted media an appropriate sanitisation method shall be deployed.

5.8.4 Types of Electronic Storage Media Applicable

- A wide range of electronic storage media may be used to store or process information including, but not necessarily limited, to:
  - Desktop computers
  - Servers
  - Multifunction devices (e.g. printers)
  - Photocopiers
  - Laptops, tablet computers and electronic notebooks
  - Mobile telephones
  - Digital recorders
  - Cameras
  - USB devices
  - DVDs, CDs and other portable devices and removable media.

5.8.5 Reuse of Electronic Media

- The type of sanitisation method deployed for a given technology will depend on the type of media and the environment/classification that it is to be re-used in. The sanitisation method shall irretrievably destroy any data held on the electronic media. If this is not possible then the media shall be destroyed.

5.8.5.1 Reuse Within the Same or Equivalent Secure Environment

- If the electronic media is to be re-used within the same secure environment and there are no “need to know” constraints, then the media may be re-used without any sanitisation. However, the existing data shall be deleted before being re-used; otherwise the media shall undergo appropriate sanitisation for the type of media as defined in the latest HMG mandatory requirements – Secure Sanitisation.

5.8.5.2 Reuse Within a Less Secure Environment

- If the electronic media is to be re-used within a less secure environment or for re-use within a non <insert name of organisation> environment, then the media shall be appropriately sanitised as defined in the latest HMG mandatory requirements – Secure Sanitisation.

5.8.6 Electronic Media Awaiting Sanitisation, Reuse or Disposal

- All electronic media awaiting disposal shall be stored and handled securely in accordance with the requirements for its classification.

5.8.7 Maintenance and Disposal by Third Parties

- Disposal of electronic media by third parties shall be in accordance with this policy and covered by assured contractual agreements.
- Faulty or unserviceable electronic media shall be appropriately sanitised in accordance with the latest HMG mandatory requirements – Secure Sanitisation before being removed for repair, replacement or disposal.
- All leased electronic media shall be sanitised in accordance with the latest HMG mandatory requirements – Secure Sanitisation before being returned to the vendor.
- All electronic media that is maintained or disposed of by third parties shall be handled appropriately as required for its classification so that there is no risk to the confidentiality of the data stored.

5.8.8 Record of Reuse and Destruction

- Where appropriate, records shall be kept documenting the asset number of the electronic media being disposed of and the method of how the media was sanitised.

5.8.9 Legal and Regulatory Requirements

- As a minimum, the Secure Sanitisation and Disposal Procedures implemented by the Trust shall meet the requirements of the following Acts and Regulations:
    - Data Protection Act 2018 or other superseding legislation – relating to the protection of personal data.
    - Caldicott Data Guardian Principles and Data Security Standards – relating to handling of personal confidential information.

- EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Waste Electrical and Electronic Equipment Regulations 2006 – relating to the disposal of electronic equipment.

5.8.10 Incident Reporting

- Release or re-use of electronic media without appropriate sanitisation shall be considered to be an information security incident and shall be reported in accordance with the Information Security Incident Policy.

5.9 Business Continuity

5.9.1 General

- The Trust Resilience Policy shall be used to enable the Trust to produce, implement, test and manage a Business Continuity Plan (management system) on the Trust IT systems to enable a structured recovery post an IT or information security incident. This document relates to the IT and information elements of the overall Trust approach to Business Continuity.

5.9.2 Business Continuity Definition

- Business Continuity is defined as the capability of the Trust to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

5.9.3 Business Continuity Approach

- The Trust shall use the "Plan-Do-Check-Act" (PDCA) model to plan, establish, implement, operate, monitor, review, maintain and continually improve the effectiveness of its Business Continuity Plan for IT and information.

5.9.4 Business Continuity Plan

- A Business Continuity Plan shall be produced to enable immediate responses to be made to an information security incident (IT or information).
- The Plan shall be regularly tested, it is suggested that this is at least annually.
- The Plan should cover:
  - Ownership – which post owns and controls the plan
  - Responsibilities – identification of roles and their responsibilities
  - Scope – what is in the plan and what is out of the plan
  - Identification of critical assets with priority order for recovery/business functionality
  - Capabilities – identified internal and external capabilities
  - Resources – allocation of tasks to resources, internal and external
  - Communication process

- Task flow – including:
    - Points of contact
    - Relationship to incident management team
    - Response actions
    - Recovery/restoration of asset or standing up of identified alternate
    - Recording of actions taken and time when assets recovered/restored.
- Post Action Review – lessons learnt.
- Test Schedule.

5.9.5 Responsibilities

- The following roles shall undertake the responsibilities listed:
    - Senior Information Risk Owner (SIRO) – coordinate the development and maintenance of the Business Continuity Plan – ensuring it relates to the overall Trust Business Continuity Strategy.
    - Head of Information Technology – maintains the Business Continuity Plan Manager on behalf of the SIRO ensuring that testing is undertaken.
    - Information Asset Owners (IAOs) – ensure that the requirements from the Business Continuity planning are adequately considered and documented for all information assets of which they have ownership; and, enable the recovery to be enacted.
    - Line Managers - ensure that staff follow the Trust Business Continuity Plan procedures.
    - Director of Information Technology – management of business continuity procedures relating to IT and information security.

5.9.6 Management and Implementation

- The Business Continuity Policy and the resulting Business Continuity Plan shall be reviewed and re-issued annually or upon identification of a change in procedure or lesson learnt.
- The effectiveness of the Policy and Plan shall be monitored through audits and tests (external and internal) and from lessons learnt during any business continuity activity.

5.9.7 Testing

- On behalf of the SIRO the Business Continuity Plan Manager shall coordinate and manage testing which should follow the below levels and is recommended to be at least annually at each level:
    - Table Top
    - Walkthrough
    - Real-time Live Test

5.10 Disaster Recovery

5.10.1 General

The Resilience Policy shall be used to enable the Trust to produce, implement, test and manage the necessary disaster recovery measures on Trust IT systems to enable a structured recovery post an IT or information loss incident.

The Trust Information Asset Owners (IAOs) and the associated Business leads, with the Senior Information Risk Owner (SIRO) shall:

- Identify, locate and prioritise NHS and other Government data/information for its importance to the Trust and the wider NHS business functions. This will be driven by the Business Continuity requirements.
- Identify the single points of failure within the Trust IT networks and IT systems.
- Identify the essential data stores, data bearers and software (operating systems and applications) for the Trust business.

- Using the above information, the Trust IAOs and the SIRO with the Director of Information Technology shall:
  - Ensure that the Trust has a comprehensive backup process that supports the identified and prioritised data stores, bearers and essential software.
  - Produce a Disaster Recovery Plan that meets the business continuity requirements and will enable forensic recovery to take place if required.
- The requirements of the Disaster Recovery Plan shall be related to the Business Continuity Plan and the Backup policy to ensure the approach is holistic.

5.10.2 Disaster Recovery Plan

- A Disaster Recovery Plan shall be produced to enable data and IT systems/functionality to be recovered in a structured and managed manner post an incident.
- The Disaster Recovery Plan shall support the requirements of Business Continuity.
- The Plan shall be regularly tested, this should be at least annually.
- The Plan should cover:
  - Ownership – which post owns and controls the plan
  - Responsibilities – identification of roles and their responsibilities
  - Identification of critical assets with priority order for recovery/business functionality
  - Capabilities – identified internal and external capabilities
  - Resources – allocation of tasks to resources, internal and external

- Task flow – including:
  - Points of contact
  - Relationship to incident management team
  - Recovery processes and actions – in a structured order
  - Recording of recovery actions taken and time when assets recovered/restored.
- Post Action Review – lessons learnt.
- Test Schedule.

5.10.3 Responsibilities

- The following roles shall undertake the responsibilities listed:
  - Senior Information Risk Owner (SIRO) – coordinate the development and maintenance of the Disaster Recovery Plan – ensuring it relates to the Trust Business Continuity Plan.
  - Head of Information Technology – maintains the Plan on behalf of the SIRO ensuring that testing is undertaken.
  - Information Asset Owners (IAOs) and Business Leads – ensure that the requirements from the Disaster Recovery planning are adequately considered and documented for all information assets of which they have ownership; and, enable the recovery to be enacted.
  - Line Managers - ensure that staff follow the Trust Disaster Recovery Plan procedures.
  - Director of Information Technolgoy – management of disaster recovery procedures relating to IT and information security.

5.10.4 Management and Implementation

- The Disaster Recovery Plan shall be reviewed and re-issued annually or upon identification of a change in procedure or lesson learnt.
- The effectiveness of the Plan shall be monitored through audits and tests (external and internal) and from lessons learnt during any business continuity activity.

5.10.5 Testing

- On behalf of the SIRO the Head of Information Technology shall coordinate and manage testing which should follow the below levels and is recommended to be at least annually at each level:
  - Table Top
  - Walkthrough
  - Real-time Live Test

5.11 <u>Social Media</u>

5.11.1 Social Media

- Social media are considered to be IT based technologies (desktop, laptop, tablet and smartphone) that allow the creating and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks.
- Social media includes, but is not limited to:
  - Facebook
  - WhatsApp
  - Messenger
  - Tumblr
  - Instagram
  - Pinterest
  - LinkedIn
  - Snapchat
  - Twitter
  - YouTube.

5.11.2 Social Media Activity

This section should be read in conjunction with the Trust Social Media Policy and Procedure.

- Only social media sites that have been authorised and enabled by the Trust IT Service operations for users shall be accessed via Trust IT systems, including via Trust issued smartphones.
- When accessing social media, including personal accounts, for personal use on Trust IT systems the following principles shall be followed by users:
  - Excessive personal use of the social media during working hours shall be forbidden and contraventions to this may lead to disciplinary action.
  - Social media shall only be used for personal activities; it is not for use for the transmission, storage or discussion of any NHS or other UK Government information.
  - Social media shall be used in a manner that does not bring the Trust or the wider NHS into disrepute or harm or tarnish its image or reputation through offensive, inappropriate or derogatory remarks.
- Where a Trust role is authorised to use social media for their responsibilities (e.g. use of Twitter, Facebook and YouTube) this shall be in accordance with the role requirements and as outlined in the job description.
- Users using social media (for personal and corporate use) shall be forbidden from:
  - Breaching data protection laws or patient confidentiality.

- Publishing images or text that might be considered as harassment or are discriminatory, offensive or abusive. This includes the promotion of discrimination based on factors such as race, sex, religion or belief, disability, sexual orientation, gender reassignment, marriage and civil partnership, pregnancy and maternity or age.
- Publishing images or text that might be considered threatening, abusive, hateful or inflammatory, which constitutes an invasion of privacy, or causes annoyance, inconvenience or needless anxiety or which promotes violence.
- Doing anything that may be considered discriminatory against, libellous or bullying and/or harassment of, any individual.
- Infringing any copyright, database right or trade mark of any other person or organisation including posting copyrighted information in a way that violates the copyright of that information.
- Publishing images or text that advocate, promote or assist in any unlawful act or any illegal activity.
- Introducing or promoting the use of any form of computer virus or malware.
- Deliberately impersonating any person, or misrepresenting your identity or affiliation with any person.
- Breaching the terms of service of the social network.
- Promoting messages for party political purposes or for campaigning organisations.
- Promoting personal financial interests or commercial ventures to secure personal advantage.
- Providing links to websites of a violent, obscene or offensive nature or which contain any content that can be construed as violating any of the above guidelines.
- Making any discriminatory, disparaging, defamatory or harassing comments or otherwise engaging in any conduct prohibited by the Trust's policies.
- Making slanderous, defamatory, false, obscene, indecent, lewd, pornographic, violent, abusive, insulting, threatening or harassing images or comments.

5.12 Bring your own device

5.12.1 Personal devices may be used for the purpose of processing NHS or other UK Government information at the users own risk. The user is expected to meet all requirements of the ICT Acceptable Use Policy and Procedure. Personal devices are not permitted to join the Trust network unless the express authorisation has been given from either the Head of Information Technology or the Director of Health Informatics. Once approved, using a personal device remains the responsibility of the end user. The Trust accepts no liability for loss or damage and therefore users should ensure they have

personal insurance to cover such use. Personal devices connected to the Trust network may be subject to forensic investigation.

5.13 WhiteBoards

Often in plain view they can pose a risk to the privacy of personal data. It is therefore important that consideration is given to the location of the board and the information posted.

Further guidance is available in the document – Management of WhiteBoards.

5.14 Telecommunications

5.14.1 General

Trust staff shall ensure that if sensitive or Official NHS or UK Government Security Classified information is to be discussed or transmitted over telecommunication devices, prior approval and authorisation shall be obtained from the Information Asset Owner (IAO) or Head of Information Governance.

Staff shall ensure that Trust issued or owned telecommunication devices are not used or moved outside Trust premises without prior approval and authorisation from the Trust's Information & Communications Technology (ICT) Management.

5.14.2 Telephone security

The identity of the caller or person called shall be established prior to disclosure of any information. This will be the responsibility of the member of Trust staff dealing with or making the telephone call.

Identity shall be established in all cases, including where the call has been transferred internally.

Where there is uncertainty over the genuineness of a caller, staff shall request the caller's telephone number, confirm its authenticity and call back. This return call should be made from another telephone where possible.

When a caller requests any information, staff shall verify the name, job title, department and organisation of the person requesting the information and the reason for the request. Staff shall consider whether it is appropriate and/or permitted for the information requested to be provided in response to a telephone request and in a telephone conversation. If in doubt, staff shall escalate to their line manager or Head of Information Governance or Data Protection Officer.

All staff shall ensure that there is no risk of telephone conversations being overheard by unauthorised persons.

When making calls that are passed to voice mail systems, staff shall ensure that no information is recorded other than name of caller and return contact telephone number.

5.14.3 Use of simple message service (SMS)

Staff who use SMS or 'text messages' for valid Trust business reasons should receive appropriate training and be made aware of expected SMS good

practice, personal accountabilities and Information Governance (IG) requirements.

Staff should avoid sending messages that could be deemed embarrassing or distressing, or that could be misinterpreted by the intended recipient.

Staff should examine carefully any text messages received as these could contain errors. Word abbreviations and other acronyms are commonly used within SMS messages as a means to maximise message content within limited text space. However, abbreviations easily understood by the author may be prone to mistyping and misinterpretation by the recipient.

Staff should delete messages from their mobile phones when they are no longer required. However, staff should consider potential IG requirements and legal obligations for the retention and storage of any message before deletion.

5.15 Fax security

5.15.1 General

Staff shall only use a fax machine to transmit information if there is no other more secure means of communication available at the time the communication is required to be made.

If use of fax is essential the following shall be considered:

Staff shall always consider whether the use of fax is the most appropriate method of sending and receiving information.

Staff shall ensure that fax machines are located where possible in a ‘Safe Haven’ or a secure environment.

When using fax to transmit information, it shall be restricted to a minimum. Only information which is essential should be included in the information transmitted.

Pre-programmed fax numbers should be regularly checked to confirm they are still valid.

A speed-dial sheet showing the fax number and the organisation allocated to each of the speed-dial keys should be displayed next to the fax machines.

5.15.2 Sending by fax

Staff shall confirm that they have the correct fax number for the recipient.

Staff shall take all reasonable steps to ensure that when a fax transmission is sent, it is received by the intended recipient.

Staff shall confirm with the intended recipient that the receiving fax machine is located in a secure area or that the intended recipient is waiting by the fax machine to receive the transmission. Staff shall request confirmation of receipt of the fax by the recipient.

Trust standard fax cover sheets shall be used with all fax transmissions. Cover sheets should show:

- Sender’s name
- Sender’s telephone number
- Sender’s fax number

- Recipient's name
- Recipient's voice number
- Recipient's fax number
- Transmission date and time
- Number of pages including the cover sheet

Staff shall ensure that cover sheets are not used to transmit information.

Staff shall confirm by telephone that the intended recipient has received the transmission.

Fax confirmation sheets shall be checked as soon as possible after transmission to confirm that the receiving fax number and number of sheets transmitted are correct.

If anything appears wrong when transmitting a fax, the call shall be suspended immediately.

If it becomes apparent that a fax has been sent to the wrong number, it shall be reported as an information security incident.

5.15.3 Receiving by fax

Staff shall ensure that documents are not left unattended at fax machines.

Fax machines should be regularly checked for unexpected received faxes.

Any incoming fax shall be handled as appropriate to its content.

If a fax is received in error, staff shall immediately notify the sender and destroy the received fax by an approved method. An incident form (see Incident Management Policy and Procedure) should be completed as soon as practicable if the fax was sent internally within the Trust.

A specific fax machine should be identified and isolated to receive faxes out of normal working hours. All other fax machines should be programmed to forward faxes to this machine.

5.16 Handheld radio security

Dependent on the type of radio used, they may be totally insecure and anything said over them may be picked up (either deliberately or accidentally) by unauthorised persons using other radio systems.

Where possible, staff shall ensure that there is no risk of radio conversations being overheard by unauthorised persons.

Only information that has been authorised to be passed via the handheld radio shall be transmitted. The radio shall be clearly labelled with the maximum level of information that will be transmitted (eg Official or Emergency).

Staff shall exercise due care and attention to safeguard the handheld radio against theft, loss or damage when it is being used.

Handheld radios shall be stored within a secure cabinet when it is not being used.

Staff shall immediately report if a handheld radio is identified as lost or stolen.

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.

3.0 Review

This policy and procedure and all its appendices will be reviewed at a minimum of once every 4 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: Information Security – Operational Security 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: 15/02/2019

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:				
Corporate Governance Assistant	31.01.2019			
Counter Fraud Specialist Manager (Tiaa)	31.01.2019			
Energy and Sustainability Manager	Not currently in post			
Chief Pharmacist and Formulary Pharmacist	Na			
Formulary Pharmacist	Na			

Staff-Side Chair	31.01.2019			
Complaints & PALS Manager	31.01.2019			
Emergency Planning team	31.01.2019	31.01.2019	Y	Y
Head of Staff Engagement and Equality	31.01.2019	04.02.2019	Y	Y
Health Records Manager	31.01.2019			
All individuals listed on the front page	31.01.2019			
All members of the Information Governance Committee	31.01.2019			
The following staff have given consent for their personal names to be included in this policy and its appendices:				
Gail Spinks, Darren Twort, Joanne Hand				

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	**Information Security – Operational Security Policy and Procedure**
What are the aims of the policy or practice?	To outline the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability 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. 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
4	Management of Whiteboards	