Liverpool Women's NHS Foundation Trust

Ref: PL005

Acceptable use of Email, Internet and Equipment

Version	3.3
Designation of Policy Author(s)	Head of Information Governance and Records
Policy Development Contributor(s)	Head of Technology
Designation of Sponsor	Chief Information Officer
Responsible Committee	Information Governance Committee
Date ratified	14/02/2023
Date Issued	01/04/2023
Review date	31/03/2024
Coverage	Trust Wide

The Trust is committed to a duty of candour by ensuring that all interactions with patients, relatives, carers, the general public, commissioners, governors, staff and regulators are honest, open, transparent and appropriate and conducted in a timely manner. These interactions be they verbal, written or electronic will be conducted in line with the NPSA, 'Being Open' alert, (NPSA/2009/PSA003 available at www.nrls.npsa.nhs.uk/beingopen and other relevant regulatory standards and prevailing legislation and NHS constitution)

It is essential in communications with patients that when mistakes are made and/or patients have a poor experience that this is explained in a plain language manner making a clear apology for any harm or distress caused.

The Trust will monitor compliance with the principles of both the duty of candour and being open NPSA alert through analysis of claims, complaints and serious untoward incidents recorded within the Ulysses Risk Management System.

CONTENTS Page

1 Executive Summary

1.1 Applicability and Scope

i. This policy covers all aspects of information within the organisation, including (but not limited to) patient/client/service user information, personnel information, organisational information

ii. This Policy covers all aspects of handing information within the organisation, including (but not limited to) structured record systems (paper and electronic) and transmission of information

iii. This Policy covers all Information systems purchased, developed and managed by/on behalf of, the organisation and any individual directly employed or any individual undertaking activity under the control or direction of the organisation

2 Introduction

i. The Trust regards all person identifiable information that it holds or processes as confidential and will implement and maintain policies to ensure compliance with all necessary mandatory obligations

ii. The Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Effective information governance plays a key part in supporting clinical governance, service planning and performance management

iii. Effective Information Governance gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.

iv. The Trust will ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management

3 Policy objectives

i. To define the standards and Trust rules for all individuals using Email, Internet and Trust equipment

4 Duties and Responsibilities

4.1 The Senior Information Risk Owner

- Is accountable for Information Governance and Information Security at a Trust level, which includes the risk assessment process for information risk, including review of annual information risk assessments that support and inform the Statement of Internal Control.
- Reviews and approve actions in respect of identified information risks
- Ensures that the organisation's approach to information risk is effective in terms of resource, commitment and execution

- Sets the overall objectives for Information Governance and Information Security for the Trust

4.2 Caldicott Guardian

- Is agreed as the 'conscience' of the organisation and to advise the Trust Board on matters relating to confidentiality.
- Reviews and approves protocols governing the disclosure of patient information across organisational boundaries.
- Approves the release of information where consent from the data subject is not considered necessary or appropriate.

4.3 Chief Information Officer

- Takes overall responsibility for IT Services for the Trust
- Ensures that the organisation complies with all mandatory requirements in respect of Information Technology, Information Security and Cyber Security
- Has overall responsibility for Information Security for the Trust
- Ensures the overall approach taken to managing Information Security, Information Systems and Information technology is appropriate
- Supports the implementation of Information Security, Information Systems and Information technology overall objectives as directed by the Senior Information Risk Owner

4.4 Head of Technology

- Is responsible for the management of Information Security across the Trust.
- Monitors local responses to Information Security incidents and provide support in developing proportionate and effective responses to manage risk.
- To be responsible, as operational Lead, for IT services and the associated security risks.
- Manages the Trust Information Technology infrastructure on a day to day basis as directed by the Chief Information Officer

5 Main Provisions

5.1 General Provisions

i. Users of the Trust equipment and systems must act reasonably and responsibly when using any Trust equipment or systems and are personally responsible for complying with all Trust Policies. Failure to comply with any Trust policy may lead to disciplinary action

ii. Users must adhere to the terms and conditions of all licencing associated with any software running on any Trust system. As well as this, users are required to comply with any lawful and any legal requirement imposed on the use of Trust systems that the Trust considers is necessary to apply.

iii. The Trust reserves the right to undertake any reasonable investigation to enforce the provisions of this policy.

5.2 Email

i. Staff are expected to ensure that, where it is necessary to transmit personal or sensitive information by Email, then staff will comply with the Caldicott Principles and ensure only the minimum amount is contained within it to achieve the specific purpose.

ii. The following disclaimer shall be added to every individuals Email, as follows:
"This email is confidential and intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of the Trust. If you are not the intended recipient, be advised that you have received this email in error and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this email in error please notify the sender. This e-mail has been checked for viruses using anti-virus software."

iii. All Emails that are sent using the Trust equipment and systems are owned by the Trust and remains the property of the Trust.

iv. The trust reserves the right to access any Email account in the Trust where it is considered reasonable and there is an operational need to do so. Where this is deemed necessary, due account will be taken of the privacy rights of the account holder.

v. Where it is considered operationally necessary to access a user's Email account then the action shall be approved by an Approving Officer.

vi. Staff are responsible for the content of any Email that they send and will be expected to ensure that the content does not breach the provisions of any Trust Policy.

vii. Staff are reminded that the Subject Access provisions of the Data Protection Act gives the right of any individual, on request and, subject to certain specific exclusions, to be given a copy of the information that the Trust holds about them, which would include the content of Emails that are about them.

viii. Where personal or sensitive information is to be E-mailed internally, then the normal Trust Email system may be used for the transmission of such information, but staff are still expected to comply with Caldicott Principles.

ix. Where personal or sensitive information is to be E-mailed externally, then an appropriate method of encryption or protection is to be used. In the unlikely event that such methods are not used, the sender will be expected to demonstrate that there was no other reasonable alternative or the information was transmitted in such a way with the express consent of the data subject.

x. The Trust does not allow users of its Email system to apply their own auto-forwarding rules.

xi. Where any individual, that has a Trust Email account, wishes to implement auto-forwarding on the Email account then this can only be implemented by the IT Department following an application to, and approval by, the IT Department. Approval for the implementation of auto-forwarding on any account shall be given by an Approving Officer

xii. Where staff receive an Email that they believe is suspicious then the Email should be immediately deleted. Where staff are unsure about whether to open an Email then they should seek advice from the IT Department

xiii. Users are expected to remain vigilant and to not open attachments that are not known to them or click on a hyperlink that is contained within an Email where there is any doubt as to the integrity of the hyperlink web address

xiv. The Trust Email account is provided for the purposes of staff carrying out their duties as an employee. The Trust discourages staff from using the Trust Email account for personal activities and reserves the right to offer no technical support to recover lost Emails where the Email that has been lost and was personal.

xv. The trust will maintain a list of domains that are considered “High Risk”, which will be overseen by the Information Governance Department and reviewed annually by the Information Governance Committee

xvi. The sending of “High Volume” Emails to “High Risk” Email domains is prohibited

xvii. Staff are not allowed to use their own personal Email address to undertake Trust business activity where such activity would ordinarily be carried out using a Trust Email address.

xviii. Individuals who are found to have sent, or have attempted to send, “High Volume” Emails to “High Risk” Emails addresses will result in that Email address being completely blocked from all outgoing Emails from that point on.

5.3 Internet

i. The Trust will, at its sole discretion, decide which Internet websites users are allowed to access and will apply automated systems to control and monitor Internet website access.

ii. The trust reserves the right to access the records of any user’s Internet activity where there is an operational need to do so. Where this is deemed necessary, the action shall be approved by an Approving Officer

5.4 Software Installation

i. No software may be loaded onto any computer at any time, unless permission has been granted from the IT Department. Once approval has been granted, the software may only be implemented under the supervision of the IT Department.

ii. Under no circumstances should software be installed on the Trust network infrastructure without the support of the IT Department. All software installation requests should be directed to IM&T for the necessary support.

iii. The Trust will neither support nor authorise the installation of software that is unlicensed, offends decency, would be considered inappropriate by any reasonable person, is not lawful or, in any way, would bring the Trust into disrepute.

iv. Staff who knowingly, or by deliberate omission of action, places the Trust Network Infrastructure, or any of its systems, at risk may be subject to disciplinary action

v. Staff are not allowed to make unauthorised copies of software and does not allow unauthorised software to be uploaded onto any of its hardware or systems. Members of staff who deliberately and knowingly installs unauthorised software may be subject to disciplinary action

vi. The Trust will assume no responsibility for any personal file that has been placed on the Trust fileservers and reserves the right to remove any such file without notice. Where the Trust requires personal information to be removed from the Trust fileserver then the request will, without undue delay, be complied with.

5.5 Use of Trust Equipment and Systems

i. Staff may use the Trust equipment and systems for personal use so long as such use:
   - Does not compromise an individual's day to day work
   - Is not excessive
   - Does not disrupt the operational activity of their department
   - Does not cause an individual to breach any of their terms and conditions of employment
   - Does not breach any Trust Policy

ii. Unless allowed for under Paragraph 5.4.iii, the Trust prohibits the use of the Trust equipment and systems where the activity relates to the following:

   - Anything unlawful
   - Supporting or running a private business
   - On-Line Gaming
   - Weapons
   - Child Abuse
   - Violence or Profanity
   - Pornography
   - Extremism or Terrorism
   - Cloud Storage or Dropbox (except those that are specifically provided by the Trust)
   - Gambling
   - Gore or other grossly offensive images
   - Filesharing Programs
   - Anything that would seek to bypass the Trust security systems or any acceptable user policy
   - Anything that promotes, facilitates or encourages hacking, data leakage, malware or other malicious activity
   - Anything within the TOR network (Dark Web)
   - Anything that would bring the Trust into disrepute

- Anything that any reasonable and rationale person would consider as offending decency

iii. Where there is a legitimate business need for any member of staff to undertake any activity that is a disallowed under Paragraph 5.4.i (above) or Paragraph 5.4.ii (above), then specific authorisation by an Approving Officer will be required. In all instances, where approval is given, a formal record of the request and the approval shall be made. Approval, if given, will be considered on a case by case basis and specific to a named individual.

iv. Staff are expected to use professional judgement at all times when using the Trust equipment and systems for personal use and will be expected, at any time, to give reasonable justification of their actions if asked to do so.

v. It is expected that staff will seek clarification from the Information Governance Department in the event of there being any doubt as whether any intended use of Trust equipment and systems is in line with this Policy. Such clarification will be sought prior to undertaking the activity in question.

vi. All activities in relation to using Trust systems and equipment will be attributable to the user account that was logged into the system at the time the activity occurred. This would apply to any system that is deployed on the Trust IT infrastructure.

vii. The Trust will assume no responsibility for any personal file that has been placed on the Trust fileservers and reserves the right to remove any such file without notice. Where the Trust requires personal information to be removed from the Trust fileserver then the request will, without undue delay, be complied with.

viii. Staff shall ensure that all remote devices are re-connected to the Trust network via direct connection or via VPN as frequently as possible but, in any case, every 90 days as a minimum.

ix. All data and software obtained from 3rd parties must be virus checked by the IT Department before being allowed to be installed on the Trust network

5.6 Remote Working

i. The Trust allows software that is licenced by the Trust to be used outside the Trust so long as the software is consistent with the conditions of the licencing of the software, although this must be undertaken with the support of IM&T Department

ii. Where staff wish to access, from a personally owned device, such as a mobile phone, any Trust information of which the Trust is the data controller, the Trust shall, at its sole discretion:

a. Impose on staff any condition or restriction that is considered necessary and appropriate. This would include, but is not limited to, requiring the installation of software on the devices themselves that is used to enable those conditions or restrictions to be enacted.
b. Deploy technology that will allow the Trust to remotely remove data from such a device as and when the Trust considers it necessary to do so and, in doing so, will

accept no responsibility for any faults that may occur on that personally owned device as a result of the deployment of such technology.

iii. Where staff do not comply, or have not agreed to comply, the Trust reserves the right to deny access to Trust information by preventing such access and to remotely removing such personal information from those personally owned devices.

iv. Where staff use their personally owned device for any Trust business activity, then staff shall ensure that:
   a. The personally owned device is kept up to date with the latest software updates
   b. The personally owned device is kept safe and secure
   c. If the personally owned device is lost, stolen, sold or is, for any other reason, no longer in the possession of the member of staff then it is reported to IT Services

v. The rights of the Trust shall extend only to personal information of which the Trust is the data controller and do not extend to any other personal information held on a personally owned device.

5.7 Trust Equipment on Loan to Staff

i. Where staff are in possession of the Trust equipment, they are personally responsible for ensuring they take reasonable care of such equipment, and it is used in line with all relevant Trust policies. Staff are not allowed to allow anyone, who is not authorised by the Trust, to be in possession of, or access, such equipment

ii. Where staff are in possession of Trust equipment and leave employment, they shall return all equipment to the Trust at the end of their employment. If the equipment is not returned to the Trust by the last day of work, then the Trust reserves the right to seek reimbursement to the value of the equipment at sufficient value for the Trust to replace the equipment

5.8 Confidential Information held on Portable Equipment

~~i.~~ Unless specifically authorised to do so by an Approving Officer, no member of staff may hold any Trust related personal confidential information on ~~a~~ removable media such as a portable hard drive or USB pen drive. Where authority has been given to hold Trust related confidential information on a portable device then the member of staff who has been authorised shall ensure that such devices are locked away when not in use.

ii. Where staff are given approval to hold any Trust related personal confidential information on removable media, as specified in Paragraph 5.8.i. (above), then staff are responsible for ensuring that any personal confidential information contained on that removable media is encrypted. The Trust will take no responsibility for the recovery of information from removable media where the personal information contained on that removable media has been encrypted by the member of staff themselves or the removable media becomes corrupted.

5.9 Bring Your Own Device (BYOD)

i. The Trust does not allow or support the use of an individual's personal device to undertake Trust business except for instances that are explicitly allowable by any Trust policy.

5.10 Accessing Trust Social Media Accounts

i. Where an employee of the Trust is given access, as an administrator, of a Trust Social Media Account, such access will be granted only to those who are approved by the Head of Communications

ii. The Trust recognises that it must comply with the password requirements of the relevant social media platform, which may make restrict or hinder the Trust's ability to apply password policies to those platforms that are in line with the Trust's internal password requirements.

iii. Due to the fact that the Trust Social Media platforms belong to the Trust itself, the Trust will allow for individuals who have access to those accounts to use a single password, which can be shared between those approved in Paragraph 5.10.i.

5.11 Access to Externally Owned and Managed Systems

i. Where an external system is either essential to the operation of the Trust, or where the Trust is obliged to use such a system and the Trust does not have managerial control of such a system, the Trust accepts that staff must comply with the password requirements of that system, which may differ from the Trust's internal password policies.

5.12 Authority to Act

i. Approving Officers are, for the purposes of this Policy:
   - Chief Information Officer
   - Head of Technology
   - Head of Information and Performance
   - Head of Information Governance and Records
   - IT Operations Manager

ii. Authority to vary from this policy for a specific reason and a time limited period can be given by an Approving Officer

iii. An Approving Officer shall not be allowed to give authority where giving such authority would give rise to a conflict of interest

iv. Authority to vary from this Policy, which is not time-limited, may initially be given by an Approving Officer but this must then be approved by the Information Governance Committee at the first opportunity

5.13 Reporting

i. The Information Governance Committee shall be informed of any incidents where the cause is a systematic failure of any of its systems of control

ii. All Managers will provide reasonable access to any system, area or individual that will allow the Information Governance Department to assess compliance to this policy through the Spot-check Programme

6 Key References

i. The Data Protection Act 2018
ii. The General Data Protection Regulations
iii. The Information Security Management NHS Code of Practice
iv. The NHS Confidentiality Code of Practice
v. The Records Management NHS Code of Practice
vi. Freedom of Information Act 2000
vii. Data Security and Protection Toolkit
viii. The Computer Misuse Act 1990

7 Associated Documents

i. All associated documents are available via the Trust Intranet at:
http://imt012/Policies_Procedures_and_Guidelines/default.aspx

ii. Procedures:
None

8 Training

i. Training for implementation of this policy is contained within the Trust overall training program and is reference by the Information Governance and Information Security Policy and Framework

9 Policy Administration

9.1 Consultation, Communication and Implementation

Consultation Required	Authorised By	Date Authorised	Comments
Impact Assessment			
GDPR	R Cowell	19/03/2018	
Have the relevant details of the 2010 Bribery Act been considered in the drafting of this policy to minimise as far as reasonably practicable the potential for bribery?	Yes		
External Stakeholders			
Trust Staff Consultation via Intranet	Start date: January 2018		End Date: January 2018

Describe the Implementation Plan for the Policy (and guideline if impacts upon policy) (Considerations include; launch event, awareness sessions, communication / training via CBU's and other management structures, etc)	By Whom will this be Delivered?
The policy is in existence already	

Version History

Date	Version	Author Name and Designation	Summary of Main Changes
21/08/2017	1.0	Russell Cowell, Head of Information Governance	Policy has been completely reviewed and re-written. Policy version set to version 1.0 to reflect the substantial changes and the fact that it has been developed as an integrated policy set
09/08/2017	1.1	Russell Cowell, Head of Head of Information Governance	Redefined and Updated KPIs. Addition of IT Operations Manager as an Approving Officer
31/03/2020	2.0	Russell Cowell, Head of Information Governance	General review and update to policy wording. Redefined categories in respect of legitimate activities when using Trust equipment, additional provisions for Bring Your own Device and staff response to suspicious Emails
04/12/2020	3.0	Russell Cowell, Head of Information Governance	General review and minor update on policy wording to make provisions clearer based on experience. Enhancements to provisions on cyber security, re-organisation of paragraphs within policies (without word changing) so some text now moved into other policies and vice versa
26/11/2021	3.1	Russell Cowell, Head of Information Governance	Policy wording updated to reflect policy decision taken by IG Committee. Paragraphs 5.2.xvi to 5.2.xviii added to policy. Paragraphs 5.6.ii to 5.6.v added to policy.
31/03/2022	3.2	Russell Cowell, Head of Information Governance	Review only and re-approval. No changes
31/03/2023	3.3	Russell Cowell, Head of Information Governance and Records	Change of sponsorship of policy to Chief Information Officer. Update on job title of Head of Information Governance to “Head of Information Governance and Records”. Addition of provisions relating to the use of personal mobile devices. Addition of provisions relating to the use of externally managed systems.

10 Initial Equality Impact Assessment Screening Tool

Name of policy/ business or strategic plans/CIP programme: **Confidentiality Policy**	**Details of policy/service/business or strategic plan/CIP programme, etc:**	
Does the policy/service/CIP/strategic plan etc affect (please tick) **Both** X		
Does the proposal, service or document affect one group more or less favourable than another on the basis of:	**Yes/No**	**Justification/evidence and data source**
Age	No	All confidential information is treated equally and all monitoring systems are neutral in terms of their application against Equality and Diversity
Disability: including learning disability, physical, sensory or mental impairment.	No	
Gender reassignment	No	
Marriage or civil partnership	No	
Pregnancy or maternity	No	
Race	No	
Religion or belief	No	
Sex	No	
Sexual orientation	No	
Human Rights – are there any issues which might affect a person's human rights?		**Justification/evidence and data source**
Right to life	No	Obligations laid out within the policy are primarily defined by the Data Protection Act. All confidential information is treated equally and all monitoring systems are neutral in terms of their application against Equality and Diversity. There would be no impact on the Human Rights as the Policy is a direct reflection of legislation, which itself would have considered the impact on Human Rights
Right to freedom from degrading or humiliating treatment	No	
Right to privacy or family life	No	
Any other of the human rights?	No	
EIA carried out by: Quality assured by: PGP Meeting	01/04/2022	Russell Cowell, Head of Information Governance