South London and Maudsley NHS Foundation Trust

IT Acceptable Use Policy

Version:	1
Ratified By:	Information Security Committee
Date Ratified:	25th June 2018
Date Policy Comes Into Effect:	26th June 2018
Author:	Deputy IG Lead & Head of Information Governance
Responsible Director:	Chief Information Officer
Responsible Committee:	Information Security Committee
Responsible Committee Approval Date:	25th June 2018
Target Audience:	All Trust Staff
Review Date:	June 2019

Equality Impact Assessment	Assessor: Deputy IG Lead	Date: 17/10/17
HRA Impact Assessment	Assessor: Deputy IG Lead	Date: 17/10/17

Document History

Version Control

Version No.	Date	Summary of Changes	Major (must go to an exec meeting) or minor changes	Author
1	1st September 2017	Initial Draft	Major	Deputy IG lead
	September 2017	Revisions and updated	Minor	Head of IG
	May 2018	Use of personal device and Secure email updated	Major	Privacy Manager
	June 2018	Updated in line with GDPR and tables dividing Acceptable and Unacceptable use	Major	Deputy IG lead

Consultation

Stakeholder/Committee/ Group Consulted	Date	Changes Made as a Result of Consultation
Information Security Committee	11/09/17	Comments, amendments and additions
Digital Services Management team	15/09/17	None
Information Security Committee	25/06/18	Amendments approved
Service Users/Carers consulted	**Date**	**Changes Made as a Result of Consultation**
Caldicott Committee	October 2017	For information – No comments receive

Plan for Dissemination of Policy

Audience(s)	Dissemination Method	Paper or Electronic	Person Responsible
All staff	Electronic, online, hardcopy	Both	Head of Communications

Key changes to policy:
Rewritten

Plan for Implementation of Policy

Details on Implementation	Person Responsible
Appropriate Use of trust system / network	All staff
Data security	Chief Information Officer

Contents

1. Introduction

This Policy sets out instructions for the acceptable use of digital information systems and services under the control of the Digital Services department and owned by South London and The Maudsley NHS Foundation Trust (SLAM).

The Acceptable Use Policy applies to all Trust staff who is a user of IT services from SLaM Digital Services, including permanent, temporary, contractors, those who are working in partnership organisations, such us South London Mental Health Partnership, King's Health Partners, other providers who have mutually arranged processes such as honorary contracts, local research authorisations such as KHP passports, research letters of access, trainees, students, public representatives, governors and volunteers. The policy also applies to third-party partners who are users of IT services from SLaM Digital Services.

The policy covers the following areas for acceptable use:

a. Use of e-mail
b. Use of the internet and the intranet
c. Use of file storage drives
d. Use of the trust network (Including passphrases/user access control)
e. Use of personal devices
f. User declaration

All end users MUST read and understand their policy as part of their mandatory information governance training (annually) as users are expected to comply with this policy as they are authorised by their line manager or supervisor to gain access to the trust IT network.

All updates to this policy will be communicated to staff by the Intranet and Yammer. Access to secure trust e-mail, N3 and the subsequent Health and Care Secure Network (HCSN), and national NHS Digital applications including the Patient Demographic Service (PDS), NHSmail are subject to the NHS terms and conditions of use and this acceptable use policy.

2. Definitions

Personal identifiable information (PII) or personal data

Personal identifiable information constitutes any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. This information includes name, address, full post code, date of birth, NHS number and Trust ID, photographs, videos, audio-tapes or other images of service users, or anything else that may be used to identify a service user directly or indirectly.

E.g. rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified

The new data protection legislation, the GDPR and the Data Protection Act 2018 have been implemented in the UK since 25 May 2018. The new legislation requires the trust to apply stricter controls to patient-level data as the data rows get longer and richer even when the data is de-identified.

Authorisation: The granting or denying of access rights to network resources, programmes or processes.

Email: The Trust network connections enable the simultaneous connection of users to both internet and e-mail services. The usage policy principles are similar.

Internet: In the context of this policy, the internet service means any online service on the web accessed via connectivity options provided by the trust, including the wired network, staff wifi, public wifi (such as wifi spark). This includes access to web sites on the www, email, social media, online networks, online and desktop apps via mobile devices, wearables and other internet connected devices. This list is not exhaustive.

Network: A system of interconnected computers which allows the exchange of information via a network connection.

Software: Computer programs, sometimes called applications

SSL: Secure Sockets Layer. These are cryptographic security protocols which provide secure communications on the Internet.

Virus: An unauthorised piece of computer code attached to a computer program which secretly copies itself using shared discs or network connections. Viruses can destroy information or make a computer inoperable.

Users: In the context of this Policy, the term 'users' or 'individuals' refers equally to employees, volunteers, governors, bank staff, contractors, students and trainees. It also includes those who are not employed by the trust but have authorised access to network, internet and email services through the IT equipment owned or managed by the trust. This includes staff of third party agencies where a formal agreement to access specific trust systems exists.

Social media: This is using a public website or an app to record an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects via networks such as Twitter, Facebook etc. Posts are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as photographs, graphics, audio or video.

Caldicott Principles: A set of standards developed in the NHS for the collection, use and confidentiality of patient related information.

CRAMM: CRAMM is a comprehensive risk assessment tool that is fully compliant with ISO 27001

Digital Services Asset: Any information system, computer programme or other equipment owned by the Trust.

Information Asset: Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation

Information Asset Owner: The member of staff responsible for an information system in the Trust, i.e. any service specific software or information system.

End User: An end user is any persons / individual that uses any computing-enabled device or appliance.

3. Purpose and Scope of the Policy

This policy sets out the responsibilities and acceptable use of IT network and information assets within the Trust.

This policy clearly defines:

- The correct and acceptable use of email, acceptable use of trust systems (code of conduct), internet and software
- Legal requirements including Data Protection Act (2018) (DPA), Freedom of Information Act (2000) (FOI) and the Regulation of Investigatory Powers Act (2000) (RIPA)
- Guidelines for good practice including the transfer of personal data
- Examples of poor practice and activities in breach of this Policy
- Monitoring and investigation processes related to email use and misuse of Trust information systems
- Managers access to a staff member's email account

Acceptable use of social media is covered in the trust media policy

Acceptable use of IT equipment is covered in the trust device policy.

4. Roles and Responsibilities

4.1. Chief Executive

Owner of the Trust infrastructure security and responsible for signing off the Trusts compliance with NHS IT Security standards.

4.2. Director of Human Resources and Organisational Development

Responsible for authorising and overseeing any investigation and disciplinary proceedings relating to the use or misuse of Trust System

4.3. Chief Information Officer (SIRO)

The Chief Information Officer is the Senior Information Risk Owner (SIRO). The SIRO is responsible for the IT Infrastructure supporting the provision of trust network and business systems. The SIRO is strategically and operationally responsible for enterprise-wide IT security and is nominated with the responsibility for the identification and management of risks to information held on Trust systems (paper or electronic) and accountable for those risks to the Trust.

4.4. Information Security Committee

Responsible for all aspects of information and technology security including:

- the technical security of the infrastructure,
- identifying possible threats relating to information security,
- the security of IT systems and processes including access control and audit,
- ensuring that the holding, processing, sharing and transfer of data meets the strict requirements of the Data Security and Protection Toolkit and complies with the Confidentiality Policy overseen by the Caldicott Committee,
- Publicising the Acceptable Use Policy.

4.5. Heads of Information Governance and IT Operational Services supported by the Deputy Information Governance Lead

Act as the Trust's IT Security Operational Team and are responsible for:

- Leading on IT security breaches investigations
- Monitoring and reporting actual or potential IT security breaches to the SIRO, Caldicott Guardian and Trust Executive team
- Ensuring security incidents are followed-up as appropriate,
- Ensuring compliance with the policy is monitored as required.

4.6. Service Directors

- Responsible for ensuring staff awareness and adherence to this Policy.

4.7. Senior Managers

- Ensuring their staff are aware of this policy and understand their responsibilities,
- Identifying and providing secure access to equipment that their staff may use to access trust network and systems
- Monitor that their staff are following this policy.

4.8. All Trust Staff

- Responsible for complying with the Acceptable Use Policy whenever they access / use the trust network and system
- must keep their network account passphrase secure,
- must only use their own login to access the network
- must report any breaches of this policy **immediately**
- must undertake annual information governance training

4.9. Digital Services

- Provide NHS Digital compliant, secure and cost-effective means of access to the Internet,
- monitor employees network activities,
- effectively manage and authorise the appropriate connection and use of the system,
- regularly review the security effectiveness of network access.

5. General Rules

Use of Non-Trust USB and removable storage device

By default, USB ports of all desktops connected to the trust networked services are disabled in line with the NHS security requirements. There are no circumstances where Digital Services can unlock any ports. Staff are advised to utilise online tools available on Microsoft Office 365 for secure mobile storage and access to files.

Acceptable Use of Trust Systems	**Unacceptable Use**
End users are expected to primarily use all trust networked services, including email, Office 365 collaboration tools, the internet, wired and Wi-Fi networks for professional	End users must NEVER use the Internet and online communication tools for any gambling, unlawful activity, including for personal business purposes

and trust business purposes. Limited and reasonable personal use is permitted as long as it does not interfere with the performance of their duties and is agreed by the line manager or supervisor. End users MUST only use the Trust's secure e-mail system @slam.nhs.uk and other O365 unified collaboration tools for business use in line with this policy	End users must NEVER use Trust email and other O365 unified collaboration tools for personal business use, unlawful activity, gambling. Users must not use and register their Trust email account for non-professional online services as this may lead to unnecessary spam email being received and compromise overall network security. End users must not 'auto-forward' emails to their personal or other business email accounts. End users must not transfer person/patient identifiable or confidential information outside the Trust via email that is not secure or upload to websites unless you are authorised to do so, or it is absolutely necessary for work purposes **Offensive, illegal and defamatory material:** End users must not under any circumstances use the e-mail system or internet facilities to access, download, send, receive or view any materials that will cause offence to any person by reason of: ○ Any sexually explicit content; ○ Any anti-semitic, biphobic, disabilist, homophobic, islamophonic, racist, sexist, transphobic material or material that could be considered defamatory or offensive on the grounds of a person's age, disability, ethnicity, gender identity, marriage or civil partnership status, nationality, pregnancy or maternity, race, religion or belief, sex or sexual orientation and political convictions. ○ Sending personal data outside the European Economic Area (United Kingdom, EU, Norway or Switzerland) without the knowledge of data subjects and necessary arrangements contravenes the Data Protection Act (2018) and guidance must be sought

	from the Information Governance Team if a request to transfer data outside the EEA is received. ○ Configuring Trust staff accounts to automatically forward email messages to a non-Trust account. ○ Sharing of e-mail passphrases. ○ Managers' requests of access to their staff's email accounts for investigations without the staff member's consent it being previously agreed with Human Resources. ○ Utilising other people's accounts to send messages without the staff member's consent to support operational duties. ○ Sending any non-business communication including jokes, political opinions, or chain emails. Any requirement for mass communication using the email system must be discussed with the Communications team. ○ Use of social media to support private or non-trust clinical and business activities on behalf of the trust

System Monitoring

The Trust may use automated content filtering software to restrict access to categories of websites that are deemed to be inappropriate, e.g. Adult/sexual, violence, criminal, etc. These are subject to on-going review. However just because you are able to access a particular website may not always mean that it is permitted. Staff are expected to follow professional code of conduct and safe online practice, avoid any gambling or unlawful website.

6. Email Use

Trust business email system is provided by SLaM Digital Services and is on the Microsoft Office 365 platform. SLaM email system used within in Trust with the format of user.name@slam.nhs.uk has been certified complaint with the NHS Digital Secure Email Standard DCB1596 (previously SCCI1596).

Emails sent to and from health and social care organisations must conform to the health and social care Secure Email Standard to ensure that sensitive and confidential information is kept secure. The Trust followed the conformance process and @slam.nhs.uk email was certified complaint with the Secure Email Standard on 28 September 2017.

This means that all emails sent from slam.nhs.uk will be sent securely but due care and attention should still be given to ensure that the recipient and information sent is correct. The guidelines below should still be adhered to at all times

Email Use Best Practice

Cyber Security and Secure Email Use

End users are regularly alerted to be vigilant and selective when clicking links embedded within emails and websites and opening email attachments.

If users are unsure about an email or its attachment, they must contact Digital Services or forward to addspam@slam.nhs.uk without opening any of the attachments or clicking on the links.

Email chains with personal data

Emails sent from one recipient to another can develop into an 'email chain' where the history of the messages sent and content of previous emails are displayed in a chain. Personal identifiable information may be inadvertently forwarded to individuals without a legitimate 'need to know' and it is the responsibility of the sender to check further down the email chain and delete any information that need not be shared.

Email with personal data about several individuals

Information about a group of service users or staff sent outside the Trust or sent into the Trust such as reports about groups of patients are deemed to be bulk personal data. Staff members intending to transmit identifiable information about several individuals for the first time should seek advice and assessment by the information.governance@slam.nhs.uk

Email Communication with Patients

The Trust encourages use of email to communicate with patients if this is the preferred route of communication with the patient and if it supports the patients' engagement in the therapeutic process. Staff must ensure that the service user agrees with this medium of communication and understands potential risks associated with e-mail security. Service users should be advised to ensure their own online security arrangements. Staff should record service users' agreement to be contacted via e-mail on ePJS in 'Managing Patient Information' section. An accurate email should be obtained from the patient and the accuracy should be checked regularly.

Reply and Reply to All Options

It is important to avoid the use of the "Reply to All" option when responding to emails. This should only be used in rare circumstances when all the original recipients need to see the response. In particular it is poor practice to get involved in an "email tennis match" (do not act impetuously – it is easy to send a harsh response to an irritating email).

Using Calendars

Calendars should be used to check, schedule and amend meetings / appointments. Staff must ensure that appointments on calendars that contain patient identifiable information is marked "Private".

Use of Distribution Lists

There are a large number of Distribution Lists already created in the Address Book. New Distribution Lists can be created in the user's Address Book. In addition, new Distribution Lists can also be created by contacting the Digital Services Desk.

If you frequently send a message to the same group(s) of people you may benefit from creating a personal Distribution List.

- Use Distribution Lists with care - is it important that everyone in that Distribution List receive the email?
- Use organisation-wide distribution lists only to communicate important business information.

The 'All SLaM Staff' distribution list is only available for use by authorised staff for exceptional trust-wide communication needs.

- If you have information which you feel would be relevant to all SLaM staff please contact the Communications Team to request for it to be published in the weekly e-News Bulletin.

Using 'Out of Office' Notifications

The 'Out of Office Assistant' notifies others of your unavailability to read your mail. This function should be set up when staff are taking annual leave, or out of the office. The Trust advises that the out of office notification should include an alternative contact and telephone number but should not include the reason for unavailability. It is considered good practice to indicate when you are likely to be available again.

Use of personal email accounts and social media

Personal email is defined as any internet email account such as Hotmail, Yahoo mail, Gmail and many other third-party services. Facebook and Twitter are examples of social networking sites.

Staff may access their personal email and social media using the Trust network provided that they have the agreement of their line manager or if reasonable personal use is allowed, it must be limited to breaks only.

For staff working from home, the Trust facilitates secure access to emails via Office 365 Outlook webmail or using remote home working (VPN) solution.

Staff must ensure that they consider appropriate use of security and privacy settings in social networking sites to protect their personal information and privacy.

Use of social media to support clinical and business activities on behalf of the Trust must always be planned thoroughly with an appraisal from the Information Governance team and the explicit permission of the Communications Department.

Further guidance on e-mail with useful tips can be found on the Digital Services Intranet page.

Staff members are expected to follow common courtesy when using email, which is outlined in the Netiquette document.

Please see the following link on https://www.yammer.com/slam.nhs.uk/#/files/95038843
https://www.yammer.com/slam.nhs.uk/#/uploaded_files/139997663?threadId=1113810947

The Trust's Equality and Diversity Policy applies to e-mail communication and must be adhered by all end users.

Acceptable use of email	**Unacceptable use of email**
Always check that you are sending information to the correct recipient. For sharing information about multiple individuals, One Drive can be used to ensure that data is sent and received safely	Do not include personal identifiable data in the subject heading Do not select multiple Distribution Lists if the information is not relevant to all the listed members. Use of email or social media to support private or non-trust clinical and business activities on behalf of the Trust Sending emails for a personal or commercial advantage/profit e.g. offering a car for sale, flat to rent or solicit to provide services for others. Sending emails to conduct a personal relationship Sending emails containing obscene or offensive words, pictures or any form of bigotry such as racism, sexism, homophobia or religious intolerance whether forwarded or initiated by a user Sending of malicious or defamatory emails to an individual or a group of individuals Staff must NEVER use personal email for: • Communication with patients, clients, service users • Any communication about patients • Any Trust business, business sensitive and in particular anything containing personal data ***The list above is not exhaustive. Such practices will be considered inappropriate use of the email system and may initiate disciplinary proceedings in accordance with the Human Resources policies.***

Email Monitoring

@slam.nhs.uk email utilises **Data Loss Prevention** policies and **retention policies** that apply automated rules on the email system to mitigate risk of data breaches. If users are alerted about an untoward breach, or when they notice an untoward action that may and has already caused a breach of this policy, users must follow the instructions of authorised Digital Services staff.

Data Loss Prevention (DLP)
DLP is an additional safeguard, implemented to the email system which will automatically encrypt any emails with enclose personal identifiable information. If the DLP is applied, you will received an email notification as below, however be assured that the email is still sent in its entirety:

This is a system generated email. Your email has been automatically encrypted as it may contain sensitive personal information. This email is for notification purposes only and requires no action. For further information please contact informationgovernance@slam.nhs.uk

Additional guidance on secure email is available on the intranet and Yammer.

7. Using the Internet and Intranet

In the context of this policy, the internet service means any online service on the web accessed via connectivity options provided by the trust, including the wired network, staff Wi-Fi, public Wi-Fi (such as Wi-Fi spark). This includes access to web sites on the www, email, social media, online networks, online and desktop apps via mobile devices, wearable and other internet connected devices. This list is not exhaustive.

Acceptable Use of Internet and Intranet	**Restrictions on Internet Use**
Users are expected to use internet resources, such as connectivity primarily for professional purposes and in support of activities in line and towards achieving the Trust's goals and objectives, Reasonable personal use of internet resources is permitted in staff members' own time, such as breaks with the prior agreement of their line manager and/or supervisor.	Creating, downloading or transmitting any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, Creating, downloading or transmitting any defamatory, offensive or otherwise unlawful images, data or other material Creating or transmitting "junk-mail" or "spam". This means unsolicited commercial webmail, chain letters or advertisements. Using the Internet to conduct private or freelance business for the purpose of commercial gain or for soliciting for personal gain or profit,

	Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other users' data or hardware or to circumvent the access controls of systems and networks of other individuals or organisations It is not appropriate for the Trust internet to be utilised for "Chat and Date" rooms or other similar purposes that are not work related. ***This is not an exclusive list and is subject to amendment.***

Monitoring of Internet Use Reporting

Anonymous monitoring of internet usage activity is requirements in order not to compromise the Trust's code of connection to the NHS secure network N3, subsequently the Statement of Compliance and the HCSN which apply to all organisations that use the health and social care network.

The terms of use of the Trust's network services are available to all Trust staff every time they log onto the network. This is displayed regularly when users login. The login compliance screen on Trust computers and on the remote access facility (VPN) provides access to the network. By users clicking on the 'I agree' button, Trust staff agrees to comply with all IT policies, including information security, information governance, confidentiality and acceptable use policies.

The Trust's security software records internet activity, including sites visited and files transferred. This is clearly indicated on the 'login compliance screen'. This information may be used should internet activity need to be reviewed in the course of investigating an incident, as part of an HR complaint of internet misuse which is to be investigated or in the event of identification of a serious breach during a routine anonymous review (e.g. Access to offensive and hostile material sites, pornography etc), such activity must be immediately reported to line managers or available senior manager. Any user who has negligently and knowingly acted in breach of the Acceptable Use policy will be subject to the Trust's disciplinary procedure

8. Official trust sites

All web sites which indicate the involvement of the Trust, (no matter how small) e.g. the use of the Trust logo, need the written consent of the Trust Communications team before they are created.

Editorial updates to such web sites are to be managed in line with guidance defined by the Trust Communications team.

9. Use of O365 and OneDrive

Users must store their work in the most appropriate place, giving due consideration to confidentiality and availability. Documents should never be stored locally (e.g. C: drive) on a desktop computer, laptop or mobile device as they are not backed up and may be irretrievably lost if the device fails or is stolen. There is also a risk that it may contain person identifiable or confidential data which could get into the wrong hands if lost or stolen.

The primary secure data storage and effective collaboration is provided by Office 365 One Drive. OneDrive has been assessed by the Digital Services and is secure provided that it is used in line with the principles of this policy. Documents saved to the network are stored in a secure area and are backed up daily.

Folders on OneDrive can be shared with specific staff members authorised by the end user. Sharing documents securely via OneDrive enables effective collaboration and is most suitable for drafting, reviewing, sharing documents. The settings can be customised to user preferences.

SLaM Digital Services advise all staff to ensure they have received adequate guidance and training to understand full set of preferences and settings.

Staff are also provided by departmental shared drives and have the access to the folder restricted by the IT department for authorised users only. Shared folders / drives are most suitable for finalised shared departmental documents that are needed for reference, such as procedures, policies, final reports. Storing information on departmental drives means that more than one person has access and the information can be retrieved in cases of unexpected leave etc.

Users must keep data storage to a minimum. Delete obsolete files on a regular basis and never store personal non-business related files on the Trust's IT equipment. Files should only be deleted in line with the NHS Records Management Code of Practice – Retention Schedules.

If a staff member leaves their post or the Trust they should ensure that any data is transferred to an appropriate colleague or their manager, as agreed with their line manager, supervisor or head of department.

10. Managers access to a staff member's email account and U Drive folder

Managers may only demand access to their staff's email accounts and U drives for investigative purposes once it has been agreed with Human Resources or Digital Services (IG).

Emails may only be checked in line with formal HR, IG investigations and policies. This cannot contravene the Human Rights Act (1998). Workers have a right to the privacy of their correspondence. All staff must be made aware if their emails are being monitored or searched.

IT Department may need to undertake email archive searches in response to subject access requests from staff and patients. The Information Security Operations Team will oversee all email searches which must match criteria defined by data subjects (requester) in line with the relevant IT process.

11. Passphrase Management

Staff must choose a passphrase that you can remember but others cannot guess: **Best passphrases are longer than 18 characters.**

Passphrase rules: **Staff must**

- Never reveal their passphrases to anyone
- Never record or write down their passphrases
- Not use the same simple passphrase: default passphrases need to be changed immediately. Passphrases that will be easy to guess, such as your significant dates or people's names should not be used.
- Not use the same passphrase for the Trust Network access elsewhere e.g. your personal social media, personal email account or shopping sites registration passphrase.
- In the event that a passphrase is forgotten, or there are suspicions that it has been discovered by a third party, the user must change their passphrase immediately or contact the Digital Service helpdesk to obtain a temporary passphrase.
- Use of another individual's account for any purpose, whether or not their passphrase was disclosed in the process, is strictly prohibited and is a disciplinary offense;
- Passphrases must be "strong", containing 18 characters, a mixture of upper and lower case letters and numeric characters.
- Neither the username nor the user's full name should be contained in the passphrase.
- To prevent unauthorised access, all workstations should be secured when left unattended, particularly those in publicly accessible areas. The use of screen lock ('Windows' and 'L' or 'Ctrl', 'Alt' and 'Delete' followed by the 'Return' key), is recommended for short periods of absence and ward based generic accounts where used. Individual user accounts should log off shared computers, if they may be called off, or absent for an extended period, particularly where other staff may need access to the workstation.
- All work (issued by the trust and those used at home) laptops must have passphrase protected start-up software installed and be encrypted to the trust standard.

12. Acceptable Network and System Usage

It is the responsibility of all users to ensure that they adhere to the instructions laid down in this policy.

Before a new user can be allocated a trust network account, they must understand and agree to the terms of this policy.

The instructions contained in the policy are special restrictions in force with regard to the Trust related computer systems and network and, are clarifications or additions to the normal security measures in force within the Trust.

All usual security precautions must be taken in addition to these specific requirements.

There are also strict NHS security requirements for Trust networks that are connected to the national NHS network by way of mandated compliance with the Data Security and Protection Toolkit.

Restrictions

Users with access to the Trust's network must not attempt or by their actions or deliberate inaction assist others to attempt

- Unauthorised access to hardware platforms
- Unauthorised introduction of software or hardware components to the network
- Unauthorised modification of network components
- Unauthorised attempts to access the Trust's network from other networks Unauthorised attempts to access other networks from within the Trust's networks
- Unauthorised circumvention of security features such as firewalls, passphrases, etc.
- Unauthorised copying or distribution of software, documentation or media associated with the Trust's IT systems

Unauthorised removal or relocation of hardware, software, documentation or media associated with the Trust's IT systems

13. Use of Personal Devices

The use of a personal device is acceptable to carry out Trust related work in various situations as outlined below.

Staff Responsibilities	**Restrictions on use of Personal Device**
It is the user's responsibility to familiarise themselves with their own device and that by using that device they agree that the Trust may require the user to install or update Trust-approved device management software. In practice, the user will be required to: ○ Prevent theft and loss of data by securing the device with biometrics; pin; password or passphrase lock. ○ Keeping information confidential by being aware of surroundings and not sharing the device with family members, friends or colleagues. ○ Keep the device software up to date. ○ Activate and use encryption services and anti-virus protection if the device features such services ○ Install and configure tracking and/or wiping services, such as Apple's 'find my phone' app, Androids 'where's my Droid' or Windows 'Find My Phone'. ○ Trust approved applications should only be used for work purposes. All Office 365 apps are approved for us, including Outlook, OneDrive, Yammer, Teams and Power BI. ○ When using the above apps, all security features must be activated included thumbprint recognition or password protection to enter the app.	Under no circumstance must personal or business sensitive data be retained on a personal device. This means the user will need to ensure that the device does not automatically download data, nor should it automatically upload to a personal cloud. **Use of Personal Cloud** Trust information must not be stored on a personal cloud for any reason. If you need to save from your personal device, then OneDrive should be used. **Loss or Stolen Device Personal Device** In the event that your device is lost or stolen, or its security is compromised, the user is required to report this to Digital Services as soon as possible, so that they can advise and assist you to change your password. You are also required to cooperate with Digital Services, which many include wiping the device remotely, even if such a wipe may result in the loss of your own data.

Monitoring of own devices

The Trust will not monitor the entire content of personal devices however, the Trust will reserve the right to monitor and log data traffic transferred between the device and the Trust systems. The user is also required to conduct all work-related online activities in line with this policy.

Support

The Trust will make all reasonable efforts to advise on how to set-up and protect personal devices to use for work purposes. However, the user has a responsibility to learn how to use and manage the device effectively.

The Trust takes no responsibility for supporting, maintaining, repairing, insuring or funding employee owned-devices, or for any damage or loss resulting from support being provided.

14. Legal Requirement

This section of the policy is intended to provide staff with information relating to the most important legal issues which may arise from their use of the e-mail system and Internet access.

These are not just theoretical issues. If the law is broken then this could lead to one or more of the following consequences:

- Civil and/or criminal liability for yourself and the Trust.
- Disciplinary action against you including your dismissal. Ignorance of the law is not a defence in court.

All network and system users are bound by the:

- Data Protection Act (2018),
- Computer Misuse Act (1990). It is a criminal offence to carry out deliberate acts designed to damage systems or data, or for a user to attempt to gain access to data that they are not authorised to access,
- Copyright, Designs and Patents Act (1999), is forbidden to copy programs and associated files without the purchase of an appropriate license. This includes downloading or using unlicensed software obtained via the Internet,

The Trust and its employees also have responsibilities under the Caldicott Guidelines and Data Protection legislation, regarding the protection and use of patient information.

Trust provided internet and Digital Service equipment must not be used to violate the laws and regulations of the United Kingdom. Use of the Trust's resources for any illegal activity constitutes disciplinary matter. Any illegal activity will be reported to the appropriate authority for future investigation.

15. Monitoring Compliance

What will be monitored i.e. measurable policy objective	Method of Monitoring	Monitoring frequency	Position responsible for performing the monitoring/ performing co-ordinating	Group(s)/committee (s) monitoring is reported to, inc responsibility for action plans and changes in practice as a result
Staff awareness	Audit	Annual	Information Governance	Information Security Committee
Staff compliance	Audit	Bi-annual	Information Governance	Information Security Committee
Technical compliance	Technical reviews	Ongoing	IT Operations	Information Security Committee
Cyber threat mitigation	Technical reviews	Ongoing	IT Operations	Information Security Committee

16. Associated Documentation

- Records Management Code of Practice for Health and Social Care 2016.
- Confidentiality Policy
- Information Security Policy
- Information Governance Policy
- Information Risk, Incident and Forensic Readiness Policy
- Secure email risk assessment

17. Freedom of Information Act 2000

All Trust policies are public documents. They will be listed on the Trusts FOI document schedule and may be requested by any member of the public under the Freedom of Information Act (2000).

Appendix 1 - Equality Impact Assessment

PART 2: Equality Impact Assessment

1. Name of policy or service development being assessed?

IT Acceptable Use Policy

2. Name of lead person responsible for the policy or service development?

Mustapha Haruna, Deputy IG Lead

3. Describe the policy or service development

What is its main aim?

The aim of the policy is to outline to all users of SLAM'S network the acceptable use of information technology systems and services under the control of the Digital Services department and owned by South London and The Maudsley NHS Foundation Trust (SLAM).

This is to ensure the organisation is protected from data security threats through the appropriate technical security of ICT equipment which supports access to, use, storage and transfer of information, and of the secure disposal of equipment once its purpose has been served.

What are its objectives and intended outcomes?

Objectives:

- Confidentiality - access to data is confined to those with the specific authority to view that data.
- Integrity - all ICT assets operating and being utilised by authorised users need to be registered with the IT Department.
- Availability - Information is available to an authorised individual in the right place at the right time.
- Protection from Information Loss – uncontrolled and unauthorised transfers of personal identifiable information presents a significant risk to the organisation.

- To ensure the implementation of physical, logical and procedural security controls for all Trust networked and non-networked devices which process or store Trust data and information.
- To ensure that controls are in place to protect the Trust IT Estate and all information assets.
- To ensure the protection of personal identifiable information both within the

boundaries of the Trust and during inbound and outbound transfer.

- To ensure that users of IT Services are aware of the regulations, standards and procedures required in providing a secure IT Service.
- To ensure the Trust works in accordance with the principles of the Data Protection Act (1998).
- To ensure all information-processing systems must be protected to minimise the risk of adverse events such as accidents, negligence and malicious damage which could jeopardise business intelligence activity, care delivery and the legal rights of both clients and staff of the Trust.

What are the main changes being made? This is a new policy, the new policy has been creating by merging the previous Email and Internet policies, alongside the additional of the use of office 365 and guidance around Cyber Security.

What is the timetable for its development and implementation? The policy was consulted with Digital Services management team and the Information Security Committee.

4. What evidence have you considered to understand the impact of the policy or service development on people with different protected characteristics

This is a revised policy that has been updated to keep it in line with national standards and the data protection legislation. The policy was consulted with Operational Directorate/boroughs and service user representatives via the Caldicott Committee when it was initially rolled out.

5. Have you explained, consulted or involved people who might be affected by the policy or service development?

N/A

6. Does the evidence you have considered suggest that the policy or service development could have a potentially positive or negative impact on equality, discrimination or good relations for people with protected characteristics?

(Please select yes or no for each relevant protected characteristic below)

Age	**Positive impact:** Yes	**Negative impact:** no

Please summarise potential impacts:

It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.

Disability	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		
Gender re-assignment	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		
Race	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		
Pregnancy & Maternity	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		
Religion and Belief	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		
Sex	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		
Sexual Orientation	**Positive impact:** Yes	**Negative impact:** No
It is anticipated the Acceptable Use policy will have a positive impact on service users by		

ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		
Marriage & Civil Partnership *(Only if considering employment issues)*	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		
Other (e.g. Carers)	**Positive impact:** Yes	**Negative impact:** No
Please summarise potential impacts: It is anticipated the Acceptable Use policy will have a positive impact on service users by ensuring that staff know the constraints and acceptable use of the Trust network / system. Therefore making service users data processed more securely.		

7. Are there changes or practical measures that you can take to mitigate negative impacts or maximise positive impacts you have identified?

N/A

8. What process has been established to review the effects of the policy or service development on equality, discrimination and good relations once it is implemented?

N/A

PART 3: Equality Impact Assessment Action plan

Potential impact	Proposed actions	Responsible/ lead person	Timescale	Progress
Review actual impact of policy	Review EIA	Policy Lead	September 2019	

Date completed: 17 /10 / 2017
Name of person completing: *Mustapha Haruna*
Operational Directorate/borough: *Corporate*
Service / Department: *Digital Service*

Appendix 2 - Human Rights Act Impact Assessment

To be completed and attached to any procedural document when submitted to an appropriate committee for consideration and approval. If any potential infringements of Human Rights are identified, i.e. by answering Yes to any of the sections below, note them in the Comments box and then refer the documents to SLaM Legal Services for further review.

For advice in completing the Assessment please contact Tony Konzon, Claims and Litigation Manager (Anthony.Konzon@slam.nhs.uk)

HRA Act 1998 Impact Assessment	Yes/No	If Yes, add relevant comments
The Human Rights Act allows for the following relevant rights listed below. Does the policy/guidance NEGATIVELY affect any of these rights?		
Article 2 - Right to Life [Resuscitation /experimental treatments, care of at risk patients]	No	
• Article 3 - Freedom from torture, inhumane or degrading treatment or punishment [physical & mental wellbeing - potentially this could apply to some forms of treatment or patient management]	No	
• Article 5 – Right to Liberty and security of persons i.e. freedom from detention unless justified in law e.g. detained under the Mental Health Act [Safeguarding issues]	No	
• Article 6 – Right to a Fair Trial, public hearing before an independent and impartial tribunal within a reasonable time [complaints/grievances]	No	
• Article 8 – Respect for Private and Family Life, home and correspondence / all other communications [right to choose, right to bodily integrity i.e. consent to treatment, Restrictions on visitors, Disclosure issues]	No	
• Article 9 - Freedom of thought, conscience and religion [Drugging patients, Religious and language issues]	No	
• Article 10 - Freedom of expression and to receive and impart information and ideas without interference. [withholding information]	No	

HRA Act 1998 Impact Assessment	Yes/No	If Yes, add relevant comments
• Article 11 - Freedom of assembly and association	No	
• Article 14 - Freedom from all discrimination	No	

Name of person completing the Initial HRA Assessment:	Deputy IG Lead
Date:	17/10/2017
Person in Legal Services completing the further HRA Assessment (if required):	
Date:	