PLEASE NOTE: Printed copies of this policy may not be the current version. Please refer to the Trust Policy Library for the current, approved version.

Policy

Acceptable Use of ICT Policy

Key Points

- The purpose of this policy is to set the 'ground rules' for the acceptable use of Information Technology systems, services and assets owned and operated by Great Ormond Street Hospital for Children NHS Trust (GOSH).
- This policy provides guidance on the use of personal devices for Trust business and sets out individuals' responsibilities.

Version:	1.5
Lead Author:	Chief Information Officer
Executive Lead:	Chief Operating Officer
Date Approved by Policy Approval Group	14 October 2019
Policy Category:	Information and Record Management
Review Date:	1 October 2022
Target Audience:	All GOSH users accessing and using Information Communication Technology (ICT) assets, as defined under section 2.

Document Control

Previous Version Information:

Previous Titles and Approval Dates:	The following policies have been consolidated: Mobile Telephone and Device Policy (23/03/15) Internet Use Policy (18/03/15) Network Access Policy (December 2017) Email Use Policy (November 2017) Encryption Policy (September 2017) Information Security Policy (May 2018)
Previous Approval Date:	(as indicated above)
Relevant to CQC requirements:	No

Relevant to Data Security and Protection Toolkit (formerly Information Governance Toolkit):	Yes
Other External Assessments	No If yes, please state which**: N/A**
Consultation:	
Individual(s) Consulted:	Chief Clinical Information Officer (CCIO), Chief Nursing Information Officer (CNIO), Chief Research Information Officer (CRIO), Information Governance Manager, ICT Security & Governance Manager, Company Secretary, Nursing Director of Operations, Director of Operational Performance and Information, Trust Solicitor
Department(s) Consulted:	Corporate Affairs, Information Governance, ICT
Committee / Group(s) Consulted:	ICT Board Operational Board
Amendments Made:	Policy re-written to consolidate the previous mobile telephone and device policy, the internet use policy, the network access policy, the email use policy, the encryption policy and the information security policy.
Keywords:	Device, Use, Internet, Email, Network, Systems, Data, Information, Security
Related Trust Documents:	
• Social Media Policy • Freedom of Information Policy • Information Governance • Data Quality Policy • Communication Policy • Confidentiality Policy • Photography, Videography and Audio Policy	

Contents

1 Introduction

1.1 This policy sets the ground rules for the acceptable use of Information Technology systems, services and assets owned and operated by Great Ormond Street Hospital for Children NHS Foundation Trust (GOSH).

1.2 The policy covers the following areas for acceptable use:

- Use of Information / Data;
- Use of e-mail;
- Use of Internet;
- Use of External Communication Tools (e.g. WhatsApp);
- Use of the Trust network & systems and remote access;
- Use of Trust and personal devices (BYOD), mobile and static;
- Use of removable media and encryption.

1.3 All staff will be required to read this policy as part of their mandatory Information Governance training.

1.4 All staff must be appropriately authorised by their manager prior to gaining access to the ICT network, services and systems.

1.5 Visiting and other temporary staff will be required to read and sign a copy of the policy before being given account credentials.

1.6 Access to the National NHS network and National applications including the NHSmail are also be subject to the NHS terms and conditions of use and their acceptable use policy.

2 Scope

2.1 This policy applies to the following staff groups:

This Acceptable Use of ICT policy applies to the following staff and or groups of people who access and use any ICT resource provided by or belonging to GOSH:

All GOSH employed staff, Board Members, Governors, Contractors, Agency staff, Honorary contract holders, Bank staff, Volunteers, Students, Observers, Young visitors programme, Work experience candidates, Foundation Year 1 & Foundation Year 2 Placements, Research Placements.

2.2 This policy does not apply to the following staff groups

None

3 Aims and Objectives

3.1 To provide clear rules about how Information Communication Technology belonging to and provided by GOSH to its staff, contractors and visitors (where applicable) must be used.

3.2 To achieve this aim, the following policy objectives must be realised:

3.2.1 Access to data shall be provided to those that need it.

3.2.2 Only authorised assets should be used for the purposes of GOSH business.

3.3 This policy embodies the Trust’s Always Values, as it requires staff to keep GOSH ICT assets safe, secure and only assessable to those who require it, contributing to our Always Expert value and it enables colleagues to work with colleagues in other teams (One Team) to deliver high quality care to patients.

4 Duties and Responsibilities

4.1 **Caldicott Guardian:** The Caldicott Guardian is responsible for agreeing and reviewing ways in which the Trust handles and discloses patient-identifiable data, making sure that the Trust is compliant with national guidance, policy and the law.

4.2 **Senior Information Risk Owner (SIRO):** The SIRO has overall responsibility for all the Trust’s Information assets and for ensuring that information risks are mitigated effectively, and as such is responsible for ensuring that this policy is in place and adhered to.

The Trust’s SIRO takes ownership of the risk management of information assets and reports as appropriate to the Trust Board..

4.3 **Information Governance Manager:** The Information Governance Manager is responsible for maintaining the Trust information asset register and managing the review process. They will also support the Trust on matters relating to the use of information ensuring compliance with the law, Trust and NHS guidelines.

4.4 **Data Protection Officer (DPO):** The Data Protection Officer is responsible for ensuring compliance of the Trust with the General Data Protection Regulations (GDPR), in particular the rights of the data subject.

4.5 **Information Asset Owners (IAO’s)**: IAO’s are operationally responsible at senior level for all information assets within their business or departmental area. IAO’s should understand and address the levels of risk in relation to the business assets they own and provide assurance to the SIRO on the security and use of those assets on at least an annual basis.

4.6 **Information Asset Administrators (IAA’s):** IAA’s work at local business or departmental levels and ensure that system administration and security procedures are in place for all information assets and that these are followed, recognised and report actual and potential security incidents, liaise with the IAO on incident management and ensure the information asset register is accurate and up to date.

4.7 **Chief Information Officer (CIO):** The CIO is responsible to ensuring the implementation of this policy.

4.8 **ICT Security & Governance Manager:** The ICT Security & Governance Manager is responsible for ensuring that all ICT systems are secure from inappropriate access.

4.9 **ICT Service:** The ICT services department is responsible for maintaining the hardware, software and security components of the ICT infrastructure and, implementing all necessary technical and physical security controls in line with the ISO 27001 Information Security Standard.

4.10 **All Trust Managers:** All managers are directly responsible for implementing policies and procedures within their business areas.

4.11 **All Trust Staff:** It is the responsibility of each employee to adhere to policies and procedures and undertake. Information Governance training on an annual basis via the Trust mandatory training and e-learning (GOLD).

5 Definitions

5.1 **Availability:** Ensuring that information is available at point of need to those authorised to access that information.

5.2 **Confidentiality**: Ensuring that personal, sensitive and/or business critical information is appropriately protected from unauthorised access and can only be accessed by those with an approved need to access that information.

5.3 **Encryption:** The process of converting information or data into a code to prevent unauthorised access

5.4 **Information Asset (data)**: Information assets are definable information resources, or data, owned or contracted by an organisation that are ‘valuable’ to the business of the organisation.

5.5 **Integrity**: Ensuring that information has not been corrupted falsely altered or otherwise changed such that it can no longer be relied upon.

5.6 **Jail Broken Device:** Removing security and software restrictions imposed by operating system providers in order to download unauthorised software.

5.7 **Malware:** Software intended to cause harm or disruption to computers or networks. There are many classifications of Malware (MALicious softWARE) but as a general term it deals with all forms of viruses, spyware, Trojans and other software designed with malicious intent

5.8 **NHS Code of Practice “Need to Know Principles”:** Access to person-identifiable or confidential information must be on a need-to-know basis and disclosure of person identifiable or confidential information must be limited to the purpose for which it is required

5.9 **Personal Identifiable Information (PII):** Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII

5.10 **Spam:** Mass unsolicited electronic mail received from an un-requested source with attempts to convince the user to purchase goods or services. SPAM consumes valuable network resources while delivering no business benefit.

5.11 **Virtual Private Network (VPN):** A system that creates a safe and encrypted connection over a less secure network, such as a public Wi-Fi or personal home connection.

6 The Policy

6.1 The principles of this policy are as follows:

6.1.1 Only ICT assets (hardware, software, information/data etc.) which are specifically authorised by the ICT Department must be used.

6.1.2 Unauthorised use, or allowing the unauthorised use of GOSH assets is strictly prohibited.

6.1.3 In addition to the requirements set under this policy, all users and the Trust are subject to the provisions of the following Acts of Parliament

- Data Protection Act 2018
- Computer Misuse Act 1990
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2001 (as amended)
- Defamation Act 2013
- Obscene Publications Act 1959
- Protection of Children Act 1999
- Equality Act 2010

Copies of these Acts and guidelines are made available via http://www.legislation.gov.uk.

6.1.4 Where it is deemed that a breach of this policy has occurred the Trust will investigate in accordance with Trust procedures. Where appropriate the Trust's disciplinary procedures will be invoked and or access to GOSH ICT systems or services may be suspended or permanently removed.

6.1.5 Where it is identified that a serious breach has occurred the Trust may take legal action (criminal or civil proceedings) in respect of this policy.

6.2 *Acceptable Use of Information (Data)*

6.2.1 Information (data) is a Trust asset. Information assets are provided for use to support GOSH with its clinical care, new and ongoing research, teaching, learning and corporate obligations.

6.2.2 The confidentiality, integrity and availability of all information stored and processed on Trust systems must remain protected at all times and only available to the right person, with the correct authority at right time in order to support our high standards of patient care and research. As defined in the NHS code of Practice, "Need to Know" Principles.

6.2.3 Users must not infringe copyright by illegally copying or distributing information.

6.2.4 Users must ensure the integrity of Trust information by adhering to the Data Quality Policy.

6.2.5 Unauthorised use and modification of information assets is strictly prohibited.

6.2.6 Where there is a genuine and reasonable need to remove information assets off-site this must be in accordance with the requirements set out in this policy under section 6.8 (removable media and encryption). Any removal of data containing Personal Identifiable Information must be authorised by an appropriate line manager.

6.2.7 If users are involved in the care of patients relating to themselves, family, friends, acquaintances, VIP's or celebrities they must advise their line manager and only access the information required in order to perform their role. Users must not, under any circumstances, access healthcare or personal information relating to the care of such patients.

6.2.8 Users must report any loss of information immediately by raising an incident on the Datix system. This includes where information has been mistakenly shared with another party, where information has accidently been lost, or where it is believed information may have been stolen from the Trust.

6.3 *Acceptable Use of Email*

6.3.1 Email will be made available to users where it is necessary to perform the duties of their role.

6.3.2 The Trust's email system is primarily a business communication tool and individuals are obliged to use it in a responsible, effective and lawful manner. The Trust allows the reasonable use of email for personal use under the following conditions:

- Personal use of email does not interfere with work or the work of others;
- Personal emails are subject to the same scrutiny and requirements of business emails, as defined under this policy;
- The forwarding of chain letters, junk mail and executables is strictly forbidden;
- Personal emails should be kept in a separate folder, named 'Private' and deleted weekly so as not to impact on the Trust system or performance;
- The Trust will not be liable for any financial or material loss to an individual when using email for personal use.

6.3.3 All emails, whether business or personal, are subject to Subject Access Requests (SAR's) and Freedom of Information Act requests (FOI's), as defined under the Data Protection Act. As such emails may be disclosed to third parties when requested under these provisions.

6.3.4 Personal Identifiable Information (PII), as defined under the Data Protection Act must not be sent by email unless it is encrypted to NHS Standards, as defined under section 6.8 of this policy.

Any information included in:

- emails to and from clinical staff that contain health information related to a patient's clinical care or treatment (including past clinical care or treatment for deceased patients)

- emails from external stakeholders (other Trusts, clinicians, parents, schools, social services etc.).

must be uploaded to the Electronic Patient Record for the relevant patient, once received. This uploading should take place promptly, and the email itself must then be deleted from the system. Emails to and from clinical staff that contain health information about a patient which are not uploaded to the EPR will be archived (see paragraph 6.3.17 below) and these emails will then be classed as misfiled.

6.3.5 Advice to and from the Legal Team (or other legal advisors) about the patient and/or family must not be uploaded to the EPR. Other examples of information that must not be uploaded to the EPR will be provided in a guideline on the intranet.

6.3.6 Users should ensure that emails are factual and accurate for the purposes of Trust business. They should not be designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.

6.3.7 Where possible clinical information should always be exchanged using the EPR Secure Chat and the use of email should be avoided where possible.

6.3.8 All emails are monitored for viruses. Users must delete any suspicious emails immediately and contact the ICT Department. If a user believes they have been compromised by a computer virus it must be reported to the ICT Department immediately.

6.3.9 You must not knowingly distribute a computer virus, harmful code or spam using the Trust's email system.

6.3.10 You must examine carefully any email coming into the organisation, including emails from known contacts, as they may contain Malware and report anything suspicious to the ICT Department.

6.3.11 The content of emails are routinely monitored. The Trust reserves the right to retain message content as required to meet legal and statutory obligations.

6.3.12 The Trust has the right to access users' email accounts at any time and has the right to disable access or change settings.

6.3.13 All email accounts and email content (business and personal) remain the property of the Trust and upon leaving the organisation users must not copy, forward or remove emails.

6.3.14 Users must not ‘auto-forward’ email to personal or other business email accounts, including NHS mail accounts such as nhs.net or nhs.uk.

6.3.15 Users must not impersonate any other user or employee when sending email.

6.3.16 Users must not amend messages received.

6.3.17 The Trust will apply an automatic archiving facility on emails, but users must ensure personal good housekeeping is adopted, as follows:

- Messages must be reviewed and deleted on a regular basis;
- If a user receives a wrongly delivered message it should be reported to the sender and the message deleted. If the email contains confidential or sensitive information the user must not use that information and must not disclose it;
- Spam or Junk emails should be deleted immediately;
- Users must be mindful of using ‘reply all’ and only use this when absolutely necessary;
- Users must not subscribe to email services which will result in e-mails being sent automatically, unless these are for the purpose of performing their role;
- Users must not send out trivial messages as these lead to congestion of the email system and reduce efficiency;
- When sending emails including previously sent messages (email chains), users must be mindful of the content and ensure that confidential or sensitive data is not being disclosed inappropriately.

6.4 *Acceptable Use of the Internet*

6.4.1 Internet access will be made available to individuals where it is necessary and useful for them to perform the duties of their role.

6.4.2 The internet is not a secure mechanism to send information to others. Users must ensure that confidential or sensitive information is not communicated on the internet.

6.4.3 The Trust will manage and monitor internet access and usage. Excessive or inappropriate usage will be investigated.

6.4.4 The Trust will restrict access to inappropriate websites as much as technology allows. However, it must not be assumed that all accessible websites are allowed, or appropriate and the following is strictly prohibited:

- Attempting to access, create, download or transmit any obscene or indecent images, data or other material;
- Attempting to access gambling or illegal activity sites;

- Creating, downloading or transmitting any defamatory, sexist, racist, offensive, terrorist related or otherwise unlawful images, data or other material;
- Creating, downloading or transmitting any material that infringes any person's intellectual property rights;
- Creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people;
- Creating or transmitting "junk-mail" or "spam". This means unsolicited commercial webmail, chain letters or advertisements;
- Using the internet for the storage or unencrypted transmission of personal identifiable information (PII);
- Using the Internet to conduct private or freelance business for the purpose of commercial gain;
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user's data or hardware;
- Placing patient identifiable information on to any internet or cloud/application storage, social media and online meetings;
- Expressing views on or of the Trust which could bring the organisation into disrepute (all external communications must adhere to the Trust's communication policy);
- Uploading of GOSH information/content/video to social media without the appropriate authority (all social media activity must adhere to the Trust's social media policy).

6.4.5 Access to the Trust's internet is primarily a business tool and staff are obliged to use it in a responsible, effective and lawful manner. The Trust allows the reasonable internet usage for personal use under the following conditions:

- Personal use of internet does not interfere with work or the work of others;
- Personal usage is subject to the same scrutiny and requirements of this policy;
- The Trust will not be liable for any financial or material loss to an individual when using the internet for personal use.

6.4.6 Users must not infringe copyright, or break the terms of licences for information, software or other material downloaded from the internet.

6.5 *Acceptable Use of External Communication Tools (e.g. WhatsApp)*

6.5.1 There are a number of external communication applications (App's) available on the market. GOSH recognises the usefulness of these tools to aid staff communication. The use of these tools is allowed where the app is fully encrypted and the information is secure (for example WhatsApp) and in certain circumstances within the Trust. However, the following rules apply:

- Personal Identifiable Information (PII) and Sensitive Personal Information (SPII) must not be communicated under any circumstances (patient, family or staff PII). PII includes any information/data that can identify an individual (this does not have to be a name or a number);
- Communication about patients, family members or staff must not be made due to:
  - A lack of transparency and lack of a record of the decision being made (to support safe clinical care and robust HR processes)
  - The potential to process personal data inadvertently via the App without individuals' consent
  - The need to access information when requested by a patient, parent or staff member.
- Only "Epic" Secure Chat should be used for clinical purposes (see paragraph 6.3.5).
- The tools can be used for general business communication at GOSH between individuals or groups, for example arranging a meeting, reminding individuals to log onto a system etc.;
- The tools may be used to advise a clinician that there is a message waiting within "Epic" Secure Chat and asking them to log in, or that an email has been sent to them. However, no PII/SPII or detail about the message should be communicated.

6.6 *Acceptable Use of the Trust Network, Systems and Remote Access*

6.6.1 Access to the Trust network will be made available to individuals where it is necessary for them to perform the duties of their role. Users will only be provided access to the network services they have been specifically authorised to use.

6.6.2 The Trust will manage and monitor network access and usage. Excessive or inappropriate usage will be investigated.

6.6.3 Users will be allocated a username and password upon being given access to the Trust network. It is their responsibility to keep these confidential.

6.6.4 Passwords are a vital security function, as such the following rules apply:

- Users must never disclose passwords to any other person, even if that person is a known colleague within the organisation;
- Passwords must meet the latest standards and users will be required to choose a compatible password;
- Users must never write a password down;
- If a user has forgotten their password, or suspect their password has been compromised they should contact the ICT Department immediately in order for it to be changed.

6.6.5 Users are responsible for the security of their ICT accounts and data and must not allow any unauthorised use.

6.6.6 Use of another individual's credentials to access the Trust network and systems is strictly prohibited.

6.6.7 ICT systems will be regularly monitored using audit trails and log files to ensure appropriate use. Where inappropriate use is identified this will be investigated and dealt with as is appropriate to the level of breach.

6.6.8 When leaving a device for a short period of time, assuming the device will not be required by another person during that time, the screen lock must be enabled to ensure the account is not compromised.

6.6.9 When leaving a device for long periods of time, leaving for the day, or where the device is required by someone else then the user must log out of the device to ensure their account is not compromised.

6.6.10 Users must not attempt to, or assist others to attempt to:

- Access hardware that they do not have access to;
- Access secure ICT rooms that they do not have access to;
- Introduce unauthorised software or hardware components to the Trust network;
- Modify or change network components;
- Access the Trust's network from an external network, unless using authorised secure remote access;
- Access external networks from the Trust's network;
- Circumvent security features such as firewalls, passwords, encryption etc.;
- Infringe copyright by copying or distributing software, documentation or media associated with the Trust's ICT systems;
- Remove or relocate hardware, software, documentation or media associated with the Trust's ICT systems.

6.6.11 Users must store work in the most appropriate location on the Trust network, giving due consideration to confidentiality and availability.

6.6.12 Documents must not be stored locally (e.g. C: Drive or Desktop) on any device (static or mobile) as they are not backed up and maybe lost if the device fails or is stolen.

6.6.13 All network resources and files remain the property of the Trust. Upon leaving the organisation users must not copy, forward or remove any files or folders from the Trust network.

6.6.14 IAA's or system managers are responsible for ensuring that access to ICT systems is strictly controlled to authorised users with the appropriate level of access permissions granted and that adequate training is provided prior to access being enabled.

6.6.15 IAA’s must ensure that access to ICT systems is regularly monitored for appropriate use and that any misuse is reported immediately to the relevant line manager, IAO or Information Governance Manager.

6.6.16 Remote access to the Trust managed networks must be authorised by the ICT Department. Only authorised devices can be used for remote access and must be configured with the necessary VPN remote access and security software by the ICT Department.

6.6.17 Remote access users should be aware of the security of their connection at any remote location (home, hotel, public hotspot or internet café). It is recommended that home wireless networks are not left on the default or supplier provided settings and should be configured to use Wi-Fi Protected Access 2 (WPA2) and AES encryption to provide the best level of protection.

6.6.18 Remote access users must ensure the safekeeping of their equipment and usernames/passwords at all times.

6.7 *Acceptable Use of Trust and Personal Devices, Mobile and Static*

6.7.1 Devices include PC’s, tablet PC’s, laptops, mobile PC’s / mobile laptops, personal digital assistants (PDA’s), mobile phones, cameras, photocopiers and or multi-functional devices (MFD’s).

6.7.2 Trust devices will be made available to individuals by the ICT Department, where it is necessary for them to perform the duties of their role.

6.7.3 Under no circumstances should individuals or departments purchase their own devices without the express approval of the ICT Department.

6.7.4 Usage of Trust devices will be monitored. Excessive usage (e.g. excessive calls and or data downloads) will be investigated.

6.7.5 If a Trust device is lost or stolen this must be reported to ICT immediately.

6.7.6 If a Trust device develops a fault this must be reported to ICT immediately.

6.7.7 If there is a requirement to move a Trust static device, a request must be made to the ICT Department. Under no circumstances should a static device be moved without the approval of the ICT Department. Where there is a requirement to move a mobile device from one department or ward another, authority to do so must be obtained by the nurse in charge / head of department.

6.7.8 The cost to replace lost, stolen or misplaced Trust devices will be covered by the directorate or department responsible for the device.

6.7.9 Where a Trust issued device is used for the purposes of photography, videography or audio recording this must be done in accordance with the specific device procedures and the Photography, Videography and Audio Policy must be fully adhered to.

6.7.10 Where an individual wishes to use a personal device for the purposes of their role (also known as Bring Your Own Device, or BYOD) they must obtain approval from their line manager and the ICT Department and they must adhere to the following rules:

- Jail Broken devices are strictly prohibited;
- The user will accept Mobile Device Management (MDM) software installed on their personal device. This will create a secure GOSH workspace and enable the ICT Department to manage that workspace remotely in the event of the device being lost or stolen;
- The workspace on the device is fully encrypted and any content or attachments can be remotely accessed by the ICT Department;
- Photos, videos and audio recordings must only be taken within the GOSH corporate workspace in accordance with the relevant procedures and must not be stored locally on the device. Under no circumstances should photos, videos or audio recordings be made and stored on the personal device itself (i.e. within the device camera role);
- Under no circumstances should a user screen shot or copy data provided within the GOSH workspace to the hard-drive of their personal device;
- Where a personal device (used for GOSH purposes) is lost or stolen it must be reported to the ICT Department immediately;
- Personally owned devices are not supported by GOSH. Staff should contact the device manufacturer or their carrier for operating system or hardware-related issues;
- If an individual has an issue using an approved GOSH application within the GOSH workspace on their personal device they can contact the ICT Service Desk for assistance;
- Individuals must adhere to all the requirements of acceptable use laid out within this policy when using their personal device for Trust purposes;
- When used for Trust business, any information received, sent or processed on the personal device within the secure GOSH workspace will be subject to FOI and Subject Access Requests;
- The Trust will not reimburse the employee for the purchase or associated costs with the device regardless of whether this was incurred during Trust business. This includes, but is not limited to; roaming charges, plan charges, overcharges, cost of applications for personal use;
- The Trust will not be liable for any financial or material loss to an individual when using their personal equipment for work purposes;
- Upon leaving the trust the individual must inform the ICT Department so that the GOSH workspace can be deleted and or GOSH accounts disabled;
- Upon changing their personal device a user must inform the ICT Department so that the work space can be wiped from the redundant device and installed on the new device.

6.8 *Acceptable Use of Removable Media and Encryption*

6.8.1 Removable media is classified as any portable device that can store and or move data, these include, but are not limited to, mobile devices (as defined in section 6.6.1 above), Universal Serial Bus (USB) Memory Sticks, Pen Drives, Floppy Disks, read/write compact disk (CD), DVD, Zip Drives, Magnetic Tapes etc.

6.8.2 GOSH data is backed up to disk and tape according to an approved backup schedule. All back-up disks and tapes must be fully encrypted to NHS Standards and the key only available to the ICT Department for the purposes of restoring data.

6.8.3 Encryption is installed by the ICT department to the following devices:

- All Trust owned laptop computers
- All portable storage devices such as USB memory sticks, hard drives, tapes etc.
- Desktop computers in open public areas
- Handheld devices such as smartphones, iPods
- Tablet devices such as tablet PC's, MCA's and iPad's
- Removable media e.g. floppy disks, CDs and DVDs
- Dictaphones and audio recordings

6.8.4 Users must not use unencrypted media of any description to store Trust or personal identifiable information. The only exception to this is where the equipment during its normal operation cannot support encryption (i.e. medical or scientific equipment). In those cases, the use of unencrypted media must be strictly controlled by that department's management and the local management will be both accountable and responsible for these devices and their use.

6.8.5 Only encrypted devices owned by the Trust may be used for the storage of personal identifiable information. The use of non-encrypted devices for storing NHS data is strictly prohibited.

6.8.6 It the responsibility of all users to ensure that where they are using mobile devices or moving data, that the data is fully encrypted in accordance with this policy. If Users are in any doubt they should contact the ICT Department for assistance.

6.8.7 Only Trust encrypted USB data sticks must be used for extracting or storing Trust and or person identifiable information. The only exception to this is noted in section 6.8.4 above.

6.8.8 USB data sticks must not be used for the creation or transmission of:

- Any material prohibited by law;
- Threatening, racist, extremist or obscene material;
- Material protected as trade secrets or copyrighted;
- Unsolicited commercial or advertising material.

6.8.9 Any person identifiable information transferred to an encrypted USB data stick must remain encrypted and must not be transferred to any other external system in an unencrypted form, except where the equipment or operating system is unable to use an encrypted data stick as noted in section 6.7.4 above.

6.8.10 If an individual choses to use their own device (BYOD) for the purposes of GOSH business, data must be created, updated and kept on a Trust supplied encrypted USB data stick. Under no circumstances should GOSH data be copied or stored to a personal or non-Trust device.

6.8.11 Data transfers are also subject to the GOSH Confidentiality Policy. The person making such a copy will be held responsible and accountable for the security of the data concerned.

6.8.12 All Trust USB encrypted sticks and files remain the property of the Trust. Upon leaving the organisation users must not copy, forward or remove any files or folders from those devices and must return them to the ICT Department along with the encryption password.

7 Training requirements

7.1 All users must complete Information Governance training and repeat it on an annual basis. Where individuals are non-compliant access to GOSH ICT Systems and Assets may be suspended.

8 Communication and Consultation

8.1 Communication will be sent to all users to advise them of the consolidation of policies into this single acceptable use policy. In addition, the policy will be incorporated as part of the Information Governance Training and all users will be required to confirm they have read and understood the policy.

8.2 Information Governance training can be found within the GOSH Online Learning & Development page (GOLD)

9 Monitoring arrangements

9.1 This section must explain how the policy will be monitored, reviewed and updated. An example is provided below.

Policy element to be monitored	Lead	Audit Tool	Frequency	Reporting arrangements (Committee or group)	Response required on any issues/recommendations identified
Incident Reporting	Information Governance Manager & ICT Security & Governance Manager	"Datix" System	Monthly	"Datix" incidents will be monitored for trends or areas of weakness and highlighted to the IG Steering Group	IG Steering Group to escalate any incidents to other relevant boards for action (e.g. ICT Board or EMT etc.)
IG Training The Trust will aim to achieve 95% of staff trained on Information Governance. A self-declaration will be included within the IG training.	Information Governance Manager	Audit	Monthly	The Information Governance Manager will report the status of IG Training to the ICT Board on a monthly basis	ICT Board to consider additional communication to achieve compliance in training ICT Board to review appropriateness of revoking access to ICT systems if low compliance continues
IG Toolkit The Trust aims to achieve and retain level 2 on each of the 45 requirements	Information Governance Manager	Audit	Monthly	The Information Governance Manager will report the status to the IG Steering Group	IG Steering Group to escalate any relevant issues for action to other relevant boards for action (e.g. ICT Board or EMT etc.)

10 Equality Impact Assessment

Equality Analysis Form – Acceptable Use of ICT Policy

Title of Document:	Acceptable Use of IT
Completed By:	Chief Information Officer
Date Completed:	October 2019
Summary of Stakeholder Feedback:	Communications and training must be accessible to all staff.

Potential Equality Impacts and Issues Identified

Protected Group	Potential Issues Identified	Actions to Mitigate / Opportunities to Promote
Age	Staff from older age groups or may be less confident accessing e-learning materials.	Regular support sessions are offered for e-learning
Disability (Including Learning Disability)	Written communication materials may not be suitable for staff with learning difficulties or visually impaired.	1:2:1 training or alternative methods of communication can be offered as required
Gender Re-Assignment	None	
Marriage or Civil Partnership	None	
Pregnancy and Maternity	None	
Race	None	
Religion or Belief	None	
Sex	None	
Sexual Orientation	None	

11 References

11.1 GOSH Social Media Policy

11.2 GOSH Freedom of Information Policy

11.3 GOSH Information Governance Policy

11.4 GOSH Data Quality Policy

11.5 GOSH Communication Policy

11.6 GOSH Confidentiality Policy

11.7 GOSH Photography, Videography and Audio policy [need to insert new name]

11.8 Data Protection Act 2018

11.9 Computer Misuse Act 1990

11.10 Human Rights Act 1998

11.11 Copyright, Designs and Patents Act 1988

11.12 Freedom of Information Act 2000

11.13 Privacy and Electronic Communications Regulations 2003

11.14 Regulation of Investigatory Powers Act 2000

11.15 Health & Social Care Act 2001 (as amended)

11.16 Defamation Act 2013

11.17 Obscene Publications Act 1959

11.18 Protection of Children Act 1999

11.19 Equality Act 2010

11.20 Copies of these Acts and guidelines are made available via http://www.legislation.gov.uk