University Hospitals of Morecambe Bay
NHS Foundation Trust

Document Type: **Policy**	**Unique Identifier:** CORP/POL/116
Document Title: **Acceptable Use Policy for Information Communication and Technology (ICT) Systems and Equipment**	**Version Number:** 4
	Status: Ratified
Scope: All UHMBT staff	**Classification:** Organisational
Author / Title: Fiona Prestwood, Information Governance Manager	**Responsibility:** Innovation, Informatics and Information
Replaces: Version 3.0, Acceptable Use Policy for ICT Systems, Corp/Pol/116	**Head of Department:** Andy Wicks, Chief Information Officer
Validated By: I3 Risk Management Forum	**Date:** 13/10/2020
Ratified By: Procedural Document and Information Leaflet Group	**Date:** 11/11/2020
Review dates may alter if any significant changes are made	**Review Date:** 01/07/2022

Which Principles of the NHS Constitution Apply? **Please list from principles 1-7 which apply** 3 Principles	**Which Staff Pledges of the NHS Constitution Apply?** **Please list from staff pledges 1-7 which apply** 3 Staff Pledges

Does this document meet the requirements of the Equality Act 2010 in relation to Race, Religion and Belief, Age, Disability, Gender, Sexual Orientation, Gender Identity, Pregnancy & Maternity, Marriage and Civil Partnership, Carers, Human Rights and Social Economic Deprivation discrimination? **Yes**

Document for Public Display: No

Reference check Joanne Phizacklea 14.8.19 (2019-2020/217)

To be completed by Library and Knowledge Services Staff

CONTENTS

BEHAVIOURAL STANDARDS FRAMEWORK

To help create a great place to work and a great place to be cared for, it is essential that our Trust policies, procedures and processes support our values and behaviours. This document, when used effectively, can help promote a workplace culture that values the contribution of everyone, shows support for staff as well as patients, recognises and celebrates the diversity of our staff, shows respect for everyone and ensures all our actions contribute to safe care and a safe working environment - all of which are principles of our Behavioural Standards Framework.

Behavioural Standards Framework – Expectations 'at a glance'

1. SUMMARY

All staff are expected to have a basic knowledge of how the Trusts' information and communication (ICT) systems and equipment function, the types of uses which are acceptable, and uses that must be avoided and are prohibited. They must be used with respect, courtesy, and responsibility, giving due regard to the priorities of the Trust Business. Systems or services used to access personal identifiable data and/or sensitive information, require staff to abide by their legal and ethical obligations, professional codes of conduct and terms of their employment

By using these systems and services, staff agree to comply with this Acceptable Use Policy (AUP).

2. PURPOSE

The Trust must put policies and procedures in place to ensure that it can fulfil all legal and regulatory obligations to maintain the security of and prevent abuse of Trust information assets.

This Acceptable Use Policy sets out the legal and regulatory requirements and the conduct expected of all users of the systems and equipment provided by the Trust. This is a key component of Information Governance and Security and applies to all information and communication systems and information technology equipment used.

3. SCOPE

This policy covers all staff including temporary workers, locums, individuals seconded or contracted from other organisations and covers the use of Trust equipment and systems in all locations, on and off site.

In this policy, UHMB or the Trust refers to University Hospitals of Morecambe Bay NHS Foundation Trust and the Innovation, Informatics, Information Service will be known as the I3 Service

In this policy Information and Communications Technology (ICT) systems or equipment, will be known as systems or equipment and are not limited to:

- Office 365 (Email, One Drive, and SharePoint)
- File and Print (Word Processing / Spread sheets / Power Point)
- Electronic patient records (EPR) /Clinical Systems
- Information Systems
- Voice over Internet Protocol telephone (VoIP)
- Social Media

In the policy, PID refers to personal identifiable data (NHS term) or personal data / special categories as per the Data Protection Act 2018 and General Data Protection Regulation and relates to both staff and patients.

4. POLICY

4.1 Roles and Responsibilities

Senior Information Risk Owner (SIRO) owns the organisation's overall information risk policy and risk assessment processes and ensures they are implemented consistently

Caldicott Guardian has responsibility for advising staff and ensure that adequate arrangements are in place to protect personal confidential data

Data Protection Officer (DPO) is responsible for ensuring the organisations compliance with data protection legislation

Information Asset Owners (IAO) are responsible for ensuring that all staff understand and apply the principles of the legislative, statutory and regulatory requirements relating to confidentiality, information security and data protection

Information Governance Team supports the Trust in maintaining and achieving the Information Governance Agenda, provide the Trust with advice and expertise on Information Governance and Information Security including information risk.

All staff are responsible for the correct use of information systems and assets, in relation to information governance and security. All staff are responsible for ensuring that confidential information is processed and stored securely and that they maintain appropriate confidentiality when using all forms of information.

4.2 Legislation and Standards

These include, but are not limited to;

- The Data Protection Act (2018)[1]
- General Data Protection Regulation (GDPR)[10]
- Human Rights Act [2]
- The Computer Misuse Act (1990)[3]
- Common Law Duty of Confidentiality[4]
- Caldicott Review (1997[5]/2013[6]/2016)[7]
- Freedom of Information Act (2000)[8]
- Confidentiality – NHS Code of Conduct (2003)[9]

If personal identifiable data is recorded in a system or equipment, the Trust and staff are responsible for ensuring that the recorded information:

- Meets legal requirements, standards and regulation such as the Data Protection Act 2018[1] (Appendix 2), Caldicott Principles (Appendix 1).

- Has a justifiable purpose
- Is accurate, complete, relevant and up to date
- Is stored securely and accessed on a 'need-to-know' basis

All staff rely on information entered into the record, so when creating or contributing to a record the individual should be vigilant, whilst there may be data checking or validation procedures in place this can never be fool proof. The individual should always contact their line manager with any concerns.

4.3 Incident Reporting, Investigation and/or resolution

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose.

Any potential or actual breaches of confidentiality must be reported to the member of staff's line manager, Information Governance department and recorded on the incident management system as soon as practicable possible.

An investigation will be conducted, either by the line manager or in conjunction with Information Governance and/ or Workforce and will reported to the appropriate governance committee. This may result in the matter being treated as a disciplinary offence and depending on severity may also be reportable to Department of Health and Information Commissioner's Office (ICO), with initial notification within 72 hours of the trust becoming aware.

Breaches reported to the ICO may result in the organisation receiving an enforcement notice or ordered to pay a monetary penalty for a serious breach of the Data Protection Legislation.

4.4 Prohibited Activities

These are deliberate activities which can or could result in;

- Corruption or unauthorised destruction of data
- Using equipment in a way that denies service to others such as overloading the network
- Wasting staff effort or computing resources including staff involved in the support of those resources

The Trust is the final arbiter on 'offensive' materials or prohibited activities, other than instances requiring criminal prosecution, this includes but is not limited to using Trust equipment, including the Internet for:

- the creation, transmission (via any means) or deliberate receipt of any images, data or other material which is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene or indecent
- private work – except where prior arrangements have been agreed
- commercial activities, including but not limited to advertising or running any sort of business
- political activities

- advertising or fund-raising for commercial or charitable organisations not directly connected with the Trust, other than social/notice board functions (i.e. public folders)
- Any other activity that would bring the Trust into disrepute.

Any user aware of or suspecting a breach must immediately alert the I3 Service Desk or report via the Trust's Incident and risk Reporting system depending on the nature of the incident.

4.5 Privacy and Monitoring of Activity

The Trust reserves the right to monitor the use of systems such as email and Internet activity, and access to Information Systems (Lorenzo) for acceptable use, investigative, disciplinary or technical purposes. These records can and will be accessed for disciplinary purposes if I3 service are so directed by a Workforce Business Partner or senior manager in the area concerned.

Any illegal activity will be reported directly to the Police, without necessarily consulting the individual and appropriate, prevailing HR disciplinary procedures will be invoked

4.6 Personal Use of Email, Internet and Storage

The Trust permits a limited level of personal use of work email but not as a substitute for a private email account or if it interferes with work commitment.

Work email is not to be used for subscription to non-work-related services and can only be used for Trust business subscriptions.

Personal web email accounts (e.g. personal Office 365, Hotmail, Gmail, doctors.org) are not to be used for work related activities.

Access to the Internet is provided for Trust business purposes (including educational purposes). This is a staff privilege not a right. Individuals can make reasonable personal use of permitted Internet sites, if it does not interfere with the performance of their duties or adversely affect system performance and is in personal time. The Trust has the final decision on deciding what constitutes excessive use.

Personal use of the Trust Instant Messaging system (Chat in MS Teams) must be kept to a minimum.

Trust document storage is provided for work purposes and should not be used for personal storage of photos, images or audio files. The I3 service reserves the right to delete personal items from Trust servers or on-line storage.

Personal on-line storage (e.g. iCloud, Drop Box) is not to be used for storing Trust PID or sensitive information .

Access to on-line storage for downloading or uploading of data (excluding PID) will be assessed and authorised on a case-by-case basis.

4.7 Office 365 on Personal Devices e.g. Smartphones

Staff are permitted to access their Trust Microsoft Office 365 account on their personal device, the device itself must not be used to record or store any PID or sensitive data this

includes images, recordings, photos of ward areas, patients and documentation, even with consent of a patient or member of staff.

Staff are responsible for downloading and updating any associated applications (apps), installing the latest security patches and having a password or PIN set on their personal device.

If a personal device is lost or stolen the I3 service desk should be informed as soon as possible so the password for the account can be either suspended or reset.

Jailbroken devices will not be permitted to access Microsoft Office 365.

4.8 Training

The Trust is committed to supporting its staff in the use of systems in a safe and secure manner.

Staff are made aware of their responsibilities for Information Governance through training provided at corporate induction, annual Core Skills Information Governance training and local induction specific to area of work.

Training in the use of a corporate or clinical system can be requested via I3 Service or via a local system administrator.

Access to Trust information systems is only permitted after successful completion of training and may also require successful completion of a competency assessment following training for example access to the Trust's Electronic Patient Record (EPR) Lorenzo.

4.9 New Access to Information Systems

For all systems a request must be made by an authorised line manager/supervisor via an I3 on-line request form or if not listed via I3 Service Desk call or identified system administrator.

For requests submitted via I3 Service, the authorising manager/supervisor will receive confirmation of account creation with a welcome email to the new users accounts outlining Trust's policies and guidelines and code of practice in relation to information systems

If at any point individuals are unsure of the process, they should contact the I3 Service Desk for advice.

Any questions are to be directed to the line manager in the first instance.

Patients and other members the public are prohibited from using these accounts and systems.

4.10 Change in Access to Information Systems

The individual user and/or their line manager is responsible for informing the I3 service of any changes to their job and ensuring system access is updated in line with these changes.

They are also responsible for handing over all files held on personal storage areas and email messages relevant to their old post to their line manager/supervisor before moving on to their new role.

Office 365 Team Owners are expected to remove them from any associated MS Teams and

should review access as a minimum annually.

4.11 Removing Access to Information Systems

The exit procedure should be followed, and all equipment returned before the individual ceases their employment with the Trust. This is the responsibility of both the individual and the appropriate line manager/supervisor. This should be done in a timely manner to ensure that the individual does not have access to Trust data through on-line accounts such as Office 365.

The individual should unsubscribe from all subscription-based email and RSS services before leaving.

Unless otherwise notified the I3 Service will delete the Office 365 (email and One-Drive) of an individual after 60 days from point of confirmation.

Any Office 365 and network accounts dormant for 60 days will be suspended until it has been verified, they are still required. Where authorised certain accounts will be retained e.g. individual classed as a 'VIP' user or where Workforce or an Executive has asked for an account to be retained. These accounts will be reviewed as a minimum on an annual basis to confirm further retention.

4.12 Authorising Access to Another Users or a Shared Email Accounts

A request should be placed via the I3 Service Desk for access to an individual or shared email and documents. Where the reason for access is confidential this can also be requested via Information Governance.

For individual accounts authorisation must be in writing (e.g. email) by the account holder, in their absence their line manager/supervisor and for some circumstance a Workforce Business Partner. From time to time, authority may be delegated for this authorisation.

For shared accounts authorisation must be granted by the 'Responsible Owner' or deputy. From time to time, authority may be delegated for this authorisation

4.13 Authorising Access to Another User's Personal One Drive Account

Individuals can grant access to folders within their personal One Drive. Where access is being granted due to absence or investigation a request should be placed via the I3 Service Desk for access. Where the reason for access is confidential this can also be requested via Information Governance.

4.14 Suspending an Account

A request should be placed via the I3 Service Desk where systems are managed by the I3 service as soon as practicable to suspend the account to stop unauthorised access or to prevent tampering or misuse, especially their Office 365 account as this is accessible on devices outside of the Trust. Where the reason for access is confidential this can also be requested via Information Governance

For all others the system administrator should be informed.

4.15 Usernames, Passwords, PINs and Smartcards

These allow access to systems and files that are applicable to the role of the individual.

Each system is set-up to enable passwords or PINs and will have differing policies to ensure the security of the system. Individuals are encouraged to base their individual password on a memorable phrase or three key words to aid recall without the need to write them down. Where possible, use a minimum of 12 characters and change at first login

Individuals should not disclose their username, password or PINs to anyone. I3 staff including I3 service desk or engineers will never ask for passwords or PINs.

Individuals are responsible for maintaining the confidentiality of the access, all activities recorded in their username, notifying the service desk of any suspected or unauthorised access.

Individuals should ensure that the account is closed at the end of each session and never leave a computer unattended (including smartcards) without logging out or activating the desktop screensaver using CTRL-ALT-DEL K or Windows Key-L. The desktop screensaver is a failsafe mechanism if an individual fail to lock the screen, not to lock after a specified time.

4.16 Smartcards

Individuals are expected to report for work with their smartcard. It is their responsibility to ensure the safety and security of their Smartcard (in the same way as a bank debit or credit card).

If an individual comes to work without the card, the manager can decide to send the individual home to collect the item within personal time. Repeated incidents could lead to further action.

'TAC' or Temporary Access Cards must only be used short term where RA support is not available. An individual should, as soon as possible, request a new smartcard or bring it to work. This includes Locums who will be complete several shifts.

Staff who are 'Responsible Owners' for TAC cards will ensure that cards are used in accordance with National RA terms and conditions, individuals complete the registration process accurately and truthfully, have up to date system (e.g. Lorenzo) and return the card at the end of the shift and not take off site

The audit trail can and will be used to identify misuse of the Smartcard. Use of TAC cards will be monitored and discrepancies or potential abuses discussed with responsible owners.

Action will be taken if it is felt that the discrepancy is a breach of policy and or terms and conditions of use

4.17 Document Storage Area (Shared drives, Teams and SharePoint)

An individual's job role and area of work defines what access they have to the Trust's secure storage.

Individuals must only store work related information in a Trust provided or approved secure location such as their personal One Drive or MS Teams

‘Download’ folder, C:\drive or a desktop are temporary storage areas and should not be used for permanent storage spaces as they not backed up and data can be easily be deleted and lost permanently

Secure document storage areas are not a replacement for or to circumvent an information system such as Lorenzo or PACs, so the storage of PID should be kept to a minimum.

Where documentation does contain PID, access should be restricted to staff ‘who need to know’ and where possible, identifiable information should keep to a minimum using the least number of identifiers e.g. RTX no / NHS no, initials and year of birth.

Only save to or work from Trust Office 365 environment, don’t download or use personal online-storage, devices or hard drives. Use a team or channel to share a document, more than one person can work on it at one time and it maintains its integrity and it is backed up.

Access to these areas should be reviewed as a minimum annually, when staff leave, move or an incident occurs.

Where files are copied from one location to another, this may inadvertently allow additional staff unauthorised access to information, be aware of its destination and who might have permission to access.

All MS Teams and their associated Channels have ‘Team Owner’ who is responsible for maintaining and managing the Team environment. They are responsible for ensure that the right people have access, checking as a minimum annually who has access. This is especially important if someone moves department and no longer needs access. They should moderate and review content in Chat, where applicable reminding staff or the trust Behaviour Standard Framework and this policy, remove documents outside of their retention period and delete unnecessary channels. They should report any inappropriate behaviours to their line management or if unable to do so Information Governance. It is also important they remind staff using their personal devices to keep them up to date.

4.18 Using Email

Everyone is responsible for the email content and attachments sent from their own inbox. This includes what might already be present in the email, the original sender has no control once it has left their inbox, so it is important not to include anything which would offend, embarrass or be disclosed unlawfully.

Emails may be disclosed under the Data Protection Act (2018)[1] (DPA) or Freedom of Information Act (2000)[8] (FoI), including deleted items. The Trust may also use email messages in legal / disciplinary proceedings

The subject heading should always reflect the content of the email which helps to prioritise and manage emails. Never mix subjects, new discussions or new email threads. Never put PID in the header. If confidential say ’Confidential’ in the subject.

Keep the content short and concise between a letter and a telephone conversation. Consider the choice of words and phrases carefully. Use **bold**, *italics*, <u>underline</u> or colour to emphasis a point. Write in lower case, CAPITALS are considered shouting, aggressive and rude. Include a signature with name, role and contact details.

Before sending any email, review could it be printed on Trust headed paper or on-line, then send, if not re-phrase or choose another method of communication.

Don't reply to all unless necessary remember the CC field is for information not necessarily action.

Do not enter into any contractual commitment by email and ensure that any emails relating to negotiation of a contract, new or existing, are marked 'subject to contract'.

Blind copy is to be only used for large distribution lists not to purposely hide or conceal recipients of the email being sent.

Auto forwarding of emails is only permitted following a risk assessment by the Information Governance Team.

Access to another individual's mailbox can only be arranged via the I3 Service Desk and must be authorised by a) the individual or b) a senior manager and agreed by a Workforce Business Partner.

Generic email accounts must have an authorised and specified purpose, defined individuals and a named manager or responsible owner. A local management protocol must be agreed and followed by all.

Abusive, obscene, discriminatory, harassing, derogatory, defamatory or otherwise inappropriate phrases or material is not acceptable under any circumstances. Any email containing offensive content as described above, must be reported to the appropriate line manager for investigation.

Forging or amending another person's email (or other electronic message) is fraud.

Individuals must manage emails in a timely and efficient manner, deal with as soon as possible in the same way as letters and telephone calls, and in accordance with any local standard for responses. Send an acknowledgement or use the 'Like' (thumbs up) emoji.

When away from work, set a professional and informative out of office message.

Individuals should create a signature that clearly identifies them which includes their name, role and contact details. Only Trust approved logs can be added to signatures.

If an email is received in error, remove any confidential information, reply to the sender only informing them of the error and that the email will be deleted from your mailbox. Use shift-delete to permanently remove and if the email contains confidential or PID then report as an incident.

Be vigilant when opening web links and attachments, be suspicious if asked to check or renew passwords and login credentials. Check the source or sender of the email, do you know them. Check for spelling or grammatical errors or look for web link that does not match what it is accessing. If you receive an email that look 'suspicious' **do not** click on any links, respond to the sender or forward. Right click and from the menu select '*Mark as junk'* or if from an external source you can '*Mark as phishing'* and report to the I3 Service Desk.

4.19 Sharing PID Using Email

Remember there is an inherent risk to sending or sharing information especially PID or confidential information outside the Trust and should be done with care and attention. Always check the email address being used, search the address book or send a test email being careful of the autofill function.

Use 'sharinglinks' instead of attaching documents, it's safer and there is more control. The

document stays secure until accessed by the recipient, access can be set so the document cannot be downloaded, access can be revoked at any time and external recipients requires a code or office 365 account to access. When access to a shared document is no longer required, manage the access by removing any permissions.

Where possible avoid PID or confidential information in the body of the email. If this email is being sent external to the Trust, it must be encrypted.

If an email is urgent or requires the recipient to respond promptly set the importance to 'High'.

Use the following table to decide support how best secure the data

Method	Share links	Body of Email
Trust staff		
Trusted Partners*		
External Services		Office 365 

**UHMB, University Hospitals of Morecambe Bay, LTHTR, Lancashire Teaching Hospital FT, LCFT, Lancashire & South Cumbria FT, ELHT, East Lancashire Hospital NHS Trust, LASCA, Primary Care Support England, SJH, St Johns Hospice, FCMS, Fylde Coast Medical(01H) Morecambe Bay CCG, Morecambe Bay Care Commissioning Group, GP Surgeries (gp-xxxxxxx.nhs.uk), NHSNW, NHS North West Leadership Academy, Midlands CSU, Commissioning Support Unit LCCSSD, BWDSSD, Blackburn with Darwin, NHS.Net, GOV.UK*

Note the use of Office 365 Encryption may incur a cost so check before using.

If you are unsure ask an Office 365 Champion, consult the Office 365 Intranet pages, contact the I3 Service Desk or Information Governance, never send an email unless you are confident you are doing it within policy

4.20 Communicating with Patients using Email

Where is it permitted and agreed it is appropriate to communicate with patients by email. A documented process should be established with key requirements. For example, sharing information leaflets or instructions or appointment dates and times.

Personal email addresses are not secure and are technically open to interception, this is why banks will not communicate confidential information to a personal email address. The Trust must take steps to protection the information, staff must understand their responsibilities and patients must be aware of their own responsibilities. Staff must gain explicit consent, which is clear and concise from the patient.

Staff should inform patients it is their responsibility to ensure that access to their email is secure including the device, particularly if they share devices and password with family members, partners and housemates

Staff should inform patients that the Trust will not email highly sensitive or confidential details to the patient's email account but may use it to request contact is made by another method e.g. telephone conversation

Staff should inform patients it is their responsibility to notify the service of any changes to

their circumstances e.g. new email address or withdrawal of consent for the information to be shared this way

Staff will ensure they get explicit consent from the patient that this method will be used, which is recorded in the patient case notes or an appropriate information system e.g. Lorenzo or EMIS.

Staff will only use the email address for the agreed purpose, include the minimal amount of personal information and where applicable send securely by sharing a document link or using Office 365 Encrypt function

4.21 Chat in Teams

Chat in Teams is a corporate tool for quick communication or correspondence between staff primarily for business purposes. It is available as a Chat or through Posts in channels.

Abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive messages are not permitted. Any inappropriate or unacceptable behaviours must be reported to the Team Owners/Champions who need to escalate through their own line management structure for investigation.

Teams owners will moderate chats in Channels.

Staff are responsible for the content of their composed or sent messages. You do not need to 'post' every day to add value to the team, it's a conversation not an obligation. When posting ask 'How will my comment make others feel when they read it'.

Avoid posting PID, an information system should be the primary record. If agreed this is an appropriate, only post the minimum amount e.g. RTX / NHS No, initials and year of birth.

Messages are stored in the Trust Office 365 storage and may be disclosed under the Data Protection Act (2018) (DPA)[1] or Freedom of Information Act (2000)[8] (FoI). The Trust reserves the right to monitor access and disclose messages. Breaches will be reported and investigated. Chats may also be used as evidence in audits and investigations.

Non-Trust approved messaging applications are not permitted on Trust devices.

4.22 Housekeeping

Staff are responsible for managing their own mailboxes and Trust personal One Drive storage. This should be done on a regular basis to actively manage and maintain a reasonable size within their allocated quota and should include deleting unwanted emails and converting emails to a PDF.

Emails should not be used as record store and a more appropriate store should be used

Staff will be notified if they are reaching their quota and can request an upgrade which will require validation and approval by their line manager, but this should not be used as an alternative solution for managing a mailbox or One Drive. Where it is found that Staff are using their mailbox as a record store, Information Governance will be informed to support the development of a more appropriate record store.

Once an email or document has been permanently deleted, the Trust does not have the ability to restore the item. This does not mean that emails and document should be kept forever. Take care when deleting emails especially if there is a rule to permanently remove

emails from your deleted items. If deleted from One Drive this will be permanently removed after 30 days.

Speak to your Office 365 Champion or consult the Office 365 Intranet help pages. If you have to keep emails intact for legal reasons and are unsure what to do contact Information Governance.

4.23 Virus and Malware Protection including Suspicious emails

Individual must take all necessary precautions and vigilant to prevent the transmission of computer viruses or malware.

All emails are routinely scanned for malware and will be quarantined by the I3 Service until corrective action is taken.

No document or file from any source outside the Trust should be used unless it has been scanned for known malware. (This process is automatic on networked PCs and laptops). This requirement covers files in any format, including removable media, CD-ROMs and email attachments.

Where possible all executable files should be installed by I3 service, downloads from the Internet should be authorised by the I3 service.

Virus or malware warning messages received in the inbox from a friend or colleague must not be forwarded to anyone as this risk could spread malware. The individual needs to contact I3 Service Desk who will determine the authenticity of the warning and establish if it is a hoax.

Emails from unexpected or unknown senders are to be treated with extreme caution. If in doubt, throw it out, shift delete and if appropriate contact the I3 service desk. Attachments or links should not be accessed. Right click and from the menu select '*Mark as junk'* or if from an external source you can '*Mark as phishing'* and report to the Service Desk.

Individuals are asked to never open an attachment unless they are sure it is genuine.

4.24 Internet

The Trust has the right to withdraw Internet access from any user and globally ban access to any inappropriate site without warning.

Unless specifically authorised, messages should not be posted under the Trust's name to any newsgroup or chat room. See guidance in Appendix 3.

Unless specifically authorised by the Trust, a website should not be published under the name of the Trust or featuring the NHS Logo.

The Trust will not accept liability for legal action resulting from staff misuse of the Internet.

Installing of executable files and plug-ins are controlled and can only be installed by the I3 service and a call should be logged with the Service Desk. Do not download unless you are absolutely certain it is permitted as it may disable the network or compromising the integrity

and security of the Trust networks and file servers. To introduce files, which cause computer problems, could be prosecutable under the Computer Misuse Act[3].

Trust device setting for cookie and cookie management are pre-defined by the Trust, these files that website use to store information about you between sessions

No member of staff is permitted to access, display or download from Internet sites anything that holds offensive material. If a user unintentionally finds they are connected to a site, which contains sexually explicit or otherwise offensive material, they must disconnect from the site immediately and inform the I3 Service Desk. Staff are reminded that following categories are blocked as they are unsuitable while others there may be a risk to the security of Trust data or network. The list of blocked categories includes but is not limited to;

- Adult/Sexually Specific
- Gambling
- Criminal Skills
- Hate Speech
- Violence
- Weapons
- Glamour & intimate apparel
- Remote proxies, filter avoidance & anonymising utilities
- Drugs, Alcohol & Tobacco
- Hacking
- Web based chat, instant messaging
- Games

There are times when access to a site is denied / blocked due to its categorisation or the content of the website assigned by the web filtering software. If the site is needed for Trust business or as part of your role within the Trust, staff must make a request for access via the I[3] Service Desk, with a clear business justification

Internet browsing is always monitored including working at home via home Internet and VPN. The Trust web filtering and monitoring software monitors and logs provide the Trust with details of your Internet Activity and retain a history of the search criteria entered

To help maintain your privacy when on the Internet

- use secure websites when connecting to services that require you enter, access PID, make sure it has the padlock symbol in the browser window and the web address begins with https://
- Log out of secure websites when you have finished your transaction, as closing the window may not automatically log you out of the site.
- Use strong passwords, change your passwords regularly and never reveal them to other people.
- Make sure your home/office Wi-Fi network is secured.
- Be careful and wary of whom you disclose personal information.
- Be cautious about who is trying to befriend you online including via email and social networks.
- Take account of the web filtering safety ratings (safety balloon)

This button...	With this color...	Indicates this...
	Green	The site is safe. If you are using Google Chrome as your browser, the button will appear as  .
	Yellow	There might be some issues with the site.
	Red	There might be some serious issues with the site.
	Gray	No rating is available for the site.
	Orange	A communication error occurred with the SiteAdvisor website that contains rating information.
	Blue	This could be an internal site or private IP range.
	White	The site is authorized by ePO administrator.
	Silver	The site is disabled by ePO administrator or policy.
	Black	The site is a phishing site. Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Only use an approved Internet Browser such as Google Chrome or Internet Explorer, the Trust maintains this on Trust devices. Requests for non-standard browser on Trust devices are approved on a case by case basis, where an appropriate business justification is provided.

4.25 Use of Social Media

The Trust uses social media as a tool to communicate in the public domain. Posting of corporate information is limited to authorised individuals.

Remember that anything posted on a social media site is in the public domain. Abide by your Professional Code(s) of Conduct and relevant Trust policies such as Data Protection and Confidentiality.

Consider the potential impact on personal reputation, the Trust and the NHS when using social media and do not bring the Trust into disrepute. For example, do not make personal (e.g. derogatory) comments about patients, colleagues, the Trust or the NHS.

Be mindful that any pictures, or comments, can be open to misinterpretation. Postings that breach a code of conduct or Trust policy could lead to disciplinary proceedings, dismissal and de-registration. See guidance in Appendix 3 for further details.

Personal devices must not be used to record or store any identifiable data (PID); this includes images, recordings, photos of ward areas, patients and documentation, even with consent of a patient or member of staff.

Photographs must not be posted if taken of any part of the hospital premises or of any staff member, patient or visitor and should not include the Trust or NHS logo with prior consent and discussion with the Communications Team.

It is not appropriate for staff to use any social media site to communicate with patients, relatives, carers to discuss or correspond regarding an individual's care or progress.

4.26 Using Digital Technology to Communicate with Patients, Staff and Other Organisations

Where possible staff should always use Trust provided equipment to communicate whether by voice call, text or video chat, as they have gone through an approval process which endeavours to ensure that the equipment is secure. A guide to appropriate apps and system to support is available in Appendix xx. Staff should abide by the restrictions on what the app or system can be used for.

Staff should familiarise themselves with the application, equipment and have a good network connection before a meeting or consultation to ensure that everything is working correctly.

Make the most of a meeting by setting agenda's and disseminating documentation prior to the meeting, including meeting etiquette.

Find a quiet space, free from background noise and if using video ensure that background is clear of confidential or sensitive information such as computer screens, whiteboards, documents and patient wristbands etc. or distractions and if needed blur the background, If on a ward and involving a patient close the best screens to make a private area or move to a private room.

Join the meeting in plenty of time especially if you are a host or chair, as you may need to admit external participants to the meeting.

Set the tone of the meeting by informing participants what is appropriate behaviour such as muting audio when not speaking, raising a virtual hand to ask a question or leaving questions to the end of the presentation. Set expectation if there is chat function as to what it can and cannot be used for such as PID. If leading or chairing the meeting be prepared to ask participants to mute themselves or ask them to re-join.

If a video consultation or call with a patient always confirm identification at the start of the call e.g. full name, date of birth and full address. Check whether they need support during the call.

If an advocate or representative (relative or carer) needs to be involved, where possible this should be arranged in advance, to confirm legitimate relationships. If not, the patient should confirm on the call they are happy to proceed or if they are unable to, the representative should confirm identification, and this should be recorded in the patients notes.

When on an audio or video call stay focused and treat the meeting as though meeting face-to-face, and where possible not get distracted by other things around such as checking your email, reading other documents that are not relevant to the meeting. If for whatever reason you need to leave early or take a call, inform the meeting via the chat function

If a personal device is to be used, staff must ensure that:

- They have enough data to complete the action as the Trust is not responsible for personal data plans or data uses, and it is completed over secure Wi-Fi
- Personal numbers are withheld and provide an alternative number
- Conversations are not recorded or used to text patients, unless you have access to an

approved platform, or it agreed this is appropriate
- Apps are download from a trusted source (Apple's Apps Store of Google Play)
- Privacy settings are reviewed and updated so data sharing is restricted and a strong password set
- Understand how apps works and tests the equipment before making any calls
- Devices and applications are kept up to date with security patched and any updates are applied when prompted
- Voice activated devices are turned off when in the vicinity

4.27 Recording meetings

Recording should not be used as a clinical record. Attend Anywhere does not have the functionality to record meetings.

Where a meeting is recorded to support minute taking or to share a presentation, all participants must be made aware at the start of the meeting and agree to the recording and dissemination. It is best practice to seek agreement in advance or before the meeting starts.

Where a meeting is recorded to support an interaction other than consultation, explicit consent must be in advance of the meeting in writing. This can be specific form or via email as long they have provided proof of identification. Recording should not be enabled during a meeting where prior agreement has not taken place.

Do not allow a recording of any type to be made against the person's wishes

All participants must be informed off the purpose of the recording, where it will be stored, who it will be shared or where it will be posted and how long it will be kept for and how it can be used. Recordings should not be used for anything other than what has been agreed and no one should feel pressured to agree or take part.

If a participant joins late and they have not given prior consent, halt the discussion and inform them of the use of recording.

Remember the recording will capture public chat, all data including annotations, poll results and notes, presenter video and audio (VoIP & telephony) and 3rd party audio. Ensure that the images or recordings do not compromise a person's privacy and dignity.

If a participant objects to a meeting being recorded, the meeting should not be recorded, or a unanimous agreement made to how it will used and shared.

If at any point a participant asks to stop or halt recorded, it should be stopped and noted in the minutes with a reason as it why, especially if it is having an adverse effect on the call.

4.28 Video Calls with patients using Non-Teams or Attend Anywhere Approved Apps

These are scenarios that have been approved on a case by case basis by Information Governance after a risk assessment has been completed.

These are currently to allow Video Calls to be made using an approved app to support patients who are isolated and unable to have visitors or for student doctors to complete

patient social histories remotely due social distancing. Only these scenarios have been approved, any other scenarios will require a risk assessment and approval by Information Governance. If unapproved this will be investigated as a breach of this policy.

Video calls must not be recorded, and a unique reference will be applied to each call and this will be deleted when no longer required.

Consent must be sort from the patient and recorded in the patients notes.

Find a quiet space, free from background noise and if using video ensure that background is clear of confidential or sensitive information such as computer screens, whiteboards, documents and patient wristbands etc. or distractions and if needed blur the background, If on a ward and involving a patient close the best screens to make a private area or move to a private room

Staff should familiarise themselves with the application, equipment and have a good network connection before a meeting or consultation to ensure that everything is working correctly.

Patients should be chaperoned to support them on the call

4.29 Patients Sharing Images and Video with the Trust

If the patient or their representative wishes to send or share a picture or video by online storage, secure email or SMS text, they can do so providing they understand that the Trust cannot guarantee the security of the file until it is saved and stored securely in the Trust IT Network.

They can share using their own on-line storage, via the Trust's Office 365 encryption function or can send a text to Trust mobile device. Personal mobile devices must not be used to receive SMS texts from patients.

If using email, the patient should also be informed as a disclaimer that the email address being used to the send the agreed picture or video and should not be used for any other correspondence and by replying they are agreeing to using this method. It should also include if not the intended recipient they should delete the email.

If using SMS text, the patient should also be informed verbally that the Trust does not control how or where phone provider stores or uses any information they gather during the call. You will download the picture and store securely and delete their number and when no longer required. In all of these cases, this should be documented in the patient's notes, the picture can be temporarily downloaded to an individual's One Drive and stored appropriately in the patients record or Trust image storage. Once verified it should be deleted from the individuals One Drive.

4.30 New Systems, Software and Applications

All new systems must be assessed by the I3 Service, where appropriate purchased through the I3 service or have prior agreement in place to meet NHS Standards.

If you wish to collect PID in a new system, or to support a new way of working, you must contact Information Governance Team first to ensure that this complies with the Data Protection and other relevant legislation and standards and the due diligence is completed. This may require a Data Protection Impact Assessment or relevant assessment completed.

All software must be purchased, installed and configured by the I3 service; this includes all software packages, software upgrades, and add-ons - however minor. It also includes shareware, freeware and any items downloaded from the internet.

Do not violate licence agreements by making illegal copies of Trust software. I3 service must authorise all software downloads from the internet or installations from CD or disc. Violation of a software licence may result in prosecution by FAST (Federation against Software Theft).

Software licensing will be arranged and recorded by the I3 service as part of the procurement and /or installation process. Any unlicensed software found on a Trust device will be automatically deleted or disabled.

Applications that provide information, such as BNF, Snomed CT are allowed but the user should make appropriate checks e.g. endorsed by a respect body or list on the NHS Health Apps library, that the information is from a respected source.

Applications that request or store personal data, are used to support treatment or used as teaching aids must be assessed for privacy and clinical safety risk with appropriate due diligence and approval before they are implemented/deployed. Contact the I3 Service in the first instance. This includes applications that are part of the Office 365 environment and are not installed as standard.

4.31 Trust Devices (PC, laptops, tablets, phones and printers)

All equipment must be purchased via the I3 service or have the prior agreement of the service to ensure that NHS standards are met. Requests can be made through the I3 service desk with appropriate authorisation.

All computers, printers and ancillary equipment used within the Trust must meet I3 standards. Acceptance of any donated or use of any non-Trust equipment must be checked by the I3 service to ensure it meets the appropriate standards

Consult the I3 service before moving any installed equipment, this will ensure that equipment is set-up correctly and asset records are updated.

Any devices no longer required should be returned to the I3 service for re-deployment or disposal.

Old equipment and backup tapes should not be disposed of by anyone other than the I3 service who will arrange for disposal in accordance with the Policy (which complies with EU Directive on Waste Electrical and Electronic Equipment).

Do not attempt to physically connect any Trust computer to any external network (either directly or via a telephone line) unless this use has been approved by the I3 Service. This includes Internet, modems, network or direct physical connection to another machine, NHS or private organisations or JANET (UK government-funded organisation computer network and related collaborative services to UK research and education).

Mobile Devices for example Laptops, can be connected to home Wi-Fi but public Wi-Fi

should be avoided where possible

By only connecting Trust equipment to an approved network avoids damage to the equipment, maintains security, prevent virus and malware infections of the Trust network and maintains our compliance with our code of connection and associated legislation (Computer Misuse Act[3] and The Data Protection Act (2018)[1])

4.32 Removable or Portable Media (data sticks, portable drives, CDROMS and digital cameras)

Use of removable media is controlled by software that defines whether a device is 'white' listed or allowed it to be written to, is excluded or is read-only.

All requests for removable media for use with Trust devices including medical devices should be made via the I3 Service, so the request can be appropriately assessed and approved for use as it has the potential to contain PID

Where personal data is to be stored on the device it should be encrypted and should be backed up to Trust storage as soon as possible and removed from the device.

Where an exception has been agreed with I3 service for unencrypted device to support the backup of the data to Trust storage, the terms and conditions of use must be abided by and the device wiped when uploaded and or removed from site.

4.33 Mobile Devices on Trust Premises

Mobile devices are restricted in areas of the Trust Premises to preserve privacy and dignity of all persons, especially where their use may disturb or disrupt others or cause an issue with medical devices.

Areas where restrictions apply will have signage which shows the type of restriction, either mobile device turned off or set to silent. All persons within the area are asked to comply.

4.34 Taking Trust Equipment Off-Site

Any equipment provided by the Trust is subject to the same conditions of use whether used at home or in the office.

The individual is responsible for taking all reasonable care and precautions to ensure safe transport and storage when moving equipment between home or other remote locations and work, keeping it locked and out of sight.

Trust equipment is not covered by the NHS insurance scheme and the individual may be held fully or partially liable for any loss, damage or theft occurring to Trust equipment whilst in their care.

Individuals may refuse to take information and equipment 'off-site' if they feel that it would be insecure and place equipment or information at risk.

All confidential documentation, whether in paper or electronic format should be stored in a

secure area of the home or any other location in which the individual is working from and stored securely during transit.

The removal of documents or equipment containing PID from site must be justified and authorised in line with that purpose.

4.35 Agile Working or Working from Home

Always **protect content from being viewed and accessed** by anyone who does not have a legitimate reason to do so. **Do not let non-Trust staff use a Trust device.**

Voice activated devices have an inherent risk that they can record conversation without people being aware, data is sometimes stored outside the UK and the data could be used by the device supplier for an intended purpose. Where possible switch off or put the device in another room so any confidential conversations are not recorded.

If in a patient's home you can ask them to switch off or put in another room, but you cannot stop the consultation if they refuse, but you must make them aware of the risk. It is their personal data and they are entitled to refuse.

Always check you have a secure and adequate Internet connection, avoid public Wi-Fi where possible. If you need to connect to a patient's Wi-Fi, you must ask their permission, but it is best to avoid where possible.

If using a personal device, only save to and work from Trust Office 365 Web environment. Do not download or use personal online storage, devices or hard drives.

If working from home contacting patients, keep the conversations discreet and confidential, close the door.

Unless you would like the patient to have your Trust mobile phone number, shield your number or use Trust provided equipment where possible to make calls to patients, as this has the ability to shield your number, so if a call is missed, they are only informed it is the NHS in Morecambe Bay and someone will ring back.

If using a personal mobile phone to speak with patients, you must shield your number.

Always take all reasonable care and precautions to ensure safe transport and storage when moving equipment between home or other remote locations and work, keeping it locked and out of sight.

4.36 Copyright

Do not infringe copyright by copying or transmitting copyright material without permission of the copyright holder ("fair use" notwithstanding). For further guidance, please contact Library & Knowledge Service. Note that if material is created as part of paid work / during employment, the copyright remains with the organisation and not the individual.

The Trust logo may be used only for official Trust documents and must be used in accordance with NHS Corporate Identity guidelines. Guidance on the application of the guidelines may be sought from the Trust's communication team.

4.37 Protecting the Trust against Cyber Crime and Fraud

Never disclose security or system access details, such as your username, password or PIN

Don't assume an email, text or phone call is authentic

Don't be rushed – a genuine organisation won't mind waiting

Listen to your instincts – you know if something doesn't feel right

Stay in control – don't panic and make a decision you'll regret

Always dispose of confidential information securely – use the confidential waste bins or shredder

Clear your desk or workstation at the end of the day – lock away personal / confidential information

Only access a record you have the legitimate or valid reason to access

Never store staff or patient information on a personal device

Never share or lend your system password or smartcard PINS, you are responsible for what is done when they are logged in

4.38 No compliance or Questions

In the event staff are unable to comply with this policy, for any reason, or have any questions they discuss firstly with their line manage or contact Information Governance (UHMB) – Information.Governance@mbhci.nhs.uk

5. ATTACHMENTS	
Number	**Title**
1	Caldicott Principles
2	Data Protection (1998) Principles
3	Social Networking Sites – Guidance for All Staff
4	Equality & Diversity Impact Assessment Tool

6. OTHER RELEVANT / ASSOCIATED DOCUMENTS The latest version of the documents listed below can all be found via the Trust Procedural Document Library intranet homepage.	
Unique Identifier	**Title and web links from the document library**
Corp/Guid/008	Use of the Internet
Corp/Pol/015	Data Protection and Confidentiality
Corp/Pol/071	Registration Authority
Corp/Pol/066	Access Control to Information Systems
I3/SOP/001	Equipment Decommissioning and Disposal
I3/SOP/003	I3 Service Backup Arrangements
Corp/Pol/048	Disciplinary Policy

7. SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS References in full	
Number	**References**
1	Great Britain (2018) Data Protection Act 2018. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 14.8.19)
2	Great Britain (1998) Human Rights Act 1998. Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents (accessed 14.8.19)
3	Great Britain (1990) Computer Misuse Act 1990. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents (accessed 14.8.19)
4	Department of Health. The Common Law Duty of Confidentiality. Available at: https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality (accessed 14.8.19)
5	Department of Health (1997) The Caldicott Committee. Report on the Review of Patient-Identifiable Information. Available from: https://webarchive.nationalarchives.gov.uk/20130124064947/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf (accessed 14.8.19)
6	National Data Guardian (2013) Caldicott review: information governance in the health and care system. Available at: https://www.gov.uk/government/publications/the-information-governance-review (accessed 14.8.19)
7	National Data Guardian (2016) Review of data security, consent and opt-outs. Available at: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs (accessed 14.8.19)
8	Great Britain (2000) Freedom of Information Act 2000. Available at: https://www.legislation.gov.uk/ukpga/2000/36/contents (accessed 14.8.19)
9	DHSC (2003). Confidentiality: NHS Code of Practice. Available from:

	www.gov.uk/government/publications/confidentiality-nhs-code-of-practice (accessed 14.8.19)
10	ICO (2018) Guide to the General Data Protection Regulation (GDPR), Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/ (accessed 14.8.19)

8. DEFINITIONS / GLOSSARY OF TERMS	
Abbreviation or Term	**Definition**
Safe Haven	A term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely.

9. CONSULTATION WITH STAFF AND PATIENTS

Enter the names and job titles of staff and stakeholders that have contributed to the document

Name	**Job Title**	**Date Consulted**
Carol Hogarth	Information Governance Analyst	24-08-2020
Gail Martin	Information Security Officer	
Sue Wightman	Privacy Officer	
Information Governance Group		
I3 Risk Management Forum		

10. DISTRIBUTION PLAN	
Dissemination lead:	Fiona Prestwood
Previous document already being used?	Yes
If yes, in what format and where?	Available in the Trust Procedural Document Library on the Trust Intranet
Proposed action to retrieve out-of-date copies of the document:	Document removed and replace with this version
To be disseminated to:	
Document Library	
Proposed actions to communicate the document contents to staff:	Include in the UHMB Weekly News – New documents uploaded to the Document Library

11. TRAINING

Is training required to be given due to the introduction of this policy? No Please delete as required

Action by	**Action required**	**Implementation Date**

12. AMENDMENT HISTORY				
Version No.	**Date of Issue**	**Page/Selection Changed**	**Description of Change**	**Review Date**
Draft version 0.1	November 2012		Draft document for consultation	
Draft version 0.2	Jan 2012		Comments from Libraries Manager and Staff Side incorporated	
Final Version 1.0	February 2012		Approved version	February 2014
1.1	May 2012		Amended Using Email Section (pgs.12-15) in line with legal comment re Data Protection Act compliance	July 2014
1.02	July 2014	Full review	Policy reviewed and updated	July 2016
2.0	November 2016	Full review	Policy reviewed and updated	November 2018
2.1	26/10/2017	Page 3	BSF page added	01/11/2018
2.2	06/07/2018	Throughout	All reference to Data Protection Act 1998 amended to the new 2018 Act	01/11/2018
2.3	22/11/2018	Review Date	Review date extended. 161/2018	01/02/2019
2.4	19/03/2019	Front Cover	Review date extended form 054/2019	01/06/2019
2.5	14/06/2019	Page 1	Review date extended form 087/2019	01/08/2019
3	01/07/2019	All	Reviewed and updated	01/07/2022
4	19/02/2020	All	Review and updated to include appropriate policy for using Office365 and cloud technologies	01/07/2022

Appendix 1: Caldicott Principles

The term Caldicott refers to a review commissioned by the Chief Medical Officer in 1997 under the chairmanship of Dame Fiona Caldicott. They investigated ways in which patient information is used in the NHS.

1. **Justify the purpose(s)** - Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use personal confidential data unless it is absolutely necessary** - Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose (s).
3. **Use the minimum necessary personal confidential data** - Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.
4. **Access to personal confidential data should be on a strict need-to-know basis** - Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. **Everyone with access to personal confidential data should be aware of their responsibilities** - Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. **Comply with the law** - Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect patient confidentiality** - Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employer.

Appendix 2: General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA18) Principles

Effective from 25 May 2018 GDPR updates and enhances the Data Protection Act 1998. Together they provide a framework for governing the handling of any personal data that the Trust uses in order to carry out its business activities and provide its services. No matter how the data is held, obtained, recorded, used or disclosed and applying to all media, the personal data must be dealt with properly to ensure compliance with these laws

Personal data shall be;

- *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').*

  The Trust must have valid reasons (known was 'lawful basis') for collecting and using personal data. The data must not be used in a way that is unduly detrimental, unexpected or misleading for the individual. The Trust must be clear, open and honest about how the personal data will be used.

- *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').*

  The Trust must be clear as purpose for using the personal data and only use for another purpose if compatible with the original purpose.

- *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

  The Trust needs to make sure that the personal data must be adequate (sufficient to fulfil the purpose), relevant (appropriate) and limited to what is necessary (do not hold more than needed)

- *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

  The Trust needs to ensure that personal data is up-to-date and complete, and where appropriate correct inaccurate or misleading data

- *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*

  The Trust must not keep the data for longer than necessary with clear retention and disposal schedules

- *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction*

or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The Trust must ensure there are appropriate security measure in place to protect the confidentiality, integrity and availability of the personal data

Additionally, the 'accountability' principle which is:

The controller shall be responsible for and be able to demonstrate compliance with the six principles.., ('accountability').

This requires the Trust to put in place appropriate measures such as policies and procedures, document activities, be able to evidence practices and regularly review and update.

Appendix 3: Social Networking Sites – Guidance for All Staff

This guidance note aims to inform staff of the Trust's position in relation to Social Networking sites. It has sourced other NHS organisational guidance, Nursing Times articles and NMC guidance, but relates to all colleagues who work with the Trust.

Many people working for the Trust use the internet at home for personal purposes, and many participate in social networking on websites such as Facebook and Twitter. Used properly, social networking sites are a great way to find old friends, join interest groups and share information. However, you should remember that anything posted on a social networking site is in the public domain. In most cases, this is uncomplicated and trouble-free. However, there are some occasions where your personal life and work life can start to overlap through these sites. For example:

- There have been occasions where patients making complaints have searched the web for information about staff involved in their care – finding social networking sites, blogs and photo galleries that could give fuel to their concerns
- Journalists increasingly use the web to research stories, and may reprint photos or comments that they find
- Some people also look on social networking sites to find out information about people applying for jobs.

As a Trust, we have no wish to interfere with your personal life. However, we would advise you, when using such sites, to consider the potential impact on both your own reputation and that of the NHS.

Areas include:

- If you make personal (e.g. derogatory) comments about patients, colleagues, the Trust or the NHS as a whole
- If you are pictured in activities, or make comments, that may be open to misinterpretation.

You should always use your own judgment but should bear in mind the codes of conduct and policies, which are part of your professional and employment requirements. Examples include:

- Professional codes of conduct (e.g. Nursing and Midwifery Council, General Medical Council, Health Professions Council)
- Relevant Trust Policies relating to data protection and confidentiality, Whistle blowing, Information Security and confidentiality clauses in your "contract" of employment.

You must not post photographs of yourself or your colleagues taken at work in the Trust, nor of patients or visitors within the Trust, nor of Trust holdings or logos. In addition, if you are aware of patients or their relatives taking photo's (either with a camera or mobile phone) then please remind them that it would be inappropriate to post these on a networking site as they may include pictures of other patients or staff.

Other useful things to consider include:

- Check your security settings on social networking site so that your information is only visible to the people who you want to see it

- Use a password that is not easy to guess – if someone does gain access to your account, they are able to see all your details, but also that of your friends
- Put your name into an internet search engine to see what people can find out about you. Are you happy with what they can see?
- Do not make friends with patients or their relatives on social networking sites, or discuss an individual's care or their progress
- Help your friends and colleagues out – let them know if you spot things on their pages that might be misconstrued.
- Do not reveal too many personal details such as contact details or your date of birth. Such information could put you at risk of identity fraud
- Health workers occasionally have to take out restraining orders on obsessive patients – so if you have any concerns, do not put yourself on a public networking site
- Do not upload any images of yourself in a work environment – these could be in breach of your code of conduct and lead to potential dismissal
- Before posting images or joining any causes, be aware that it is not just your friends and colleagues who may see this, but also patients and employers
- What may be considered to be 'letting off steam' about a situation at work can potentially be read by someone who may take offence at the content of a posting.

Registered staff could be putting their registration at risk if posting inappropriate comments about colleagues or patients or posting any material that could be considered explicit.

Appendix 4: Communicating with Staff, Patients and other Organisations.

Tool	*Device*	*Type*	*UHMB*	*Patients*	*Other NHS Trusts*	*Other professionals*
Cisco Phone		Voice				
Microsoft Teams		Voice Message Video				
Trust Email		Message		Only send information	Send a link or encrypt if PID	Send a link or encrypt if PID
Mobile Phone*		Voice		Withhold no for personal & Trust where appropriate		
Attend Anywhere**		Video	Use Microsoft Teams			
Jitsi Meet		Video		Do not record Patient relatives only		
WhatsApp*		Voice Video	Use Microsoft Teams	Can't withhold no Remove contacts & messages Consent to use		
Skype*		Video	Use Microsoft Teams	Can't withhold no Remove contacts & messages Consent to use		

*Its good practice to create a script to support the calls ** This is currently being tested in small groups as a proof of concept

PC/Laptop	Headphones	Trust Mobile	Personal Mobile	iPad	OK	OK with caveats	Not to be used

Appendix 5: Equality & Diversity Impact Assessment Tool

University Hospitals of Morecambe Bay NHS Foundation Trust

Equality Impact Assessment Form

Department/Function	Information Governance	
Lead Assessor	Fiona Prestwood – Information Governance Manager	
What is being assessed?	Acceptable Use Policy for ICT Systems and Equipment	
Date of assessment	01-07-2019	
What groups have you consulted with? Include details of involvement in the Equality Impact Assessment process.	Network for Inclusive Healthcare?	NO
	Staff Side Colleague?	NO
	Service Users?	NO
	Staff Inclusion Network(s)?	NO
	Personal Fair Diverse Champions?	NO
	Other (including external organisations):	

1) **What is the impact on the following equality groups?**

Positive:	**Negative:**	**Neutral:**
➢ Advance Equality of opportunity ➢ Foster good relations between different groups ➢ Address explicit needs of Equality target groups	➢ Unlawful discrimination / harassment / victimisation ➢ Failure to address explicit needs of Equality target groups	➢ It is quite acceptable for the assessment to come out as Neutral Impact. ➢ Be sure you can justify this decision with clear reasons and evidence if you are challenged

Equality Groups	**Impact** (Positive / Negative / Neutral)	**Comments** ➢ Provide brief description of the positive / negative impact identified benefits to the equality group. ➢ Is any impact identified intended or legal?
Race (All ethnic groups)	Neutral	
Disability (Including physical and mental impairments)	Neutral	
Sex	Neutral	
Gender reassignment	Neutral	
Religion or Belief	Neutral	
Sexual orientation	Neutral	
Age	Neutral	
Marriage and Civil Partnership	Neutral	
Pregnancy and maternity	Neutral	

Other (e.g. caring, human rights)	Neutral	

2) In what ways does any impact identified contribute to or hinder promoting equality and diversity across the organisation?	

3) If your assessment identifies a negative impact on Equality Groups you must develop an action plan **to avoid discrimination and ensure opportunities for promoting equality diversity and inclusion are maximised.**

- This should include where it has been identified that further work will be undertaken to further explore the impact on equality groups
- This should be reviewed annually.

Action Plan Summary

Action	**Lead**	**Timescale**

This form will be automatically submitted for review for Policies and Procedures once approved by Policy Group. For all other assessments, please return an electronic copy to EIA.forms@mbht.nhs.uk once completed.