

**Computer Use Policy**

IT1 Information Technology Policies

April 2025

**Contents**

[1 Introduction 2](#_Toc164089536)

[2 Scope and Purpose 2](#_Toc164089537)

[3 Definitions 3](#_Toc164089538)

[4 Acceptable IT Usage 4](#_Toc164089539)

[5 Passwords 9](#_Toc164089540)

[6 End User Device Security 13](#_Toc164089541)

[7 Anti-Virus and Anti Malware 16](#_Toc164089542)

[8 Wi Fi 18](#_Toc164089543)

[9 File Management and Storage 20](#_Toc164089544)

[10 IT Exception Policy and Procedure 22](#_Toc164089545)

[11 Approved Software 24](#_Toc164089546)

[12 Roles and Responsibilities 25](#_Toc164089547)

[13 Training and Monitoring 27](#_Toc164089548)

[14 Communication and Dissemination 27](#_Toc164089549)

[15 EDI Impact Assessments 28](#_Toc164089550)

[16 Resources 28](#_Toc164089551)

[17 Appendices 28](#_Toc164089552)

[Appendix 1: Exception Request Form 28](#_Toc164089553)

[Appendix 2: Approved Applications List 29](#_Toc164089554)

[18 Version Control 32](#_Toc164089555)

1. Introduction
   1. This policy covers computer usage (including laptops, smart phones, and tablets), computer networks, software programs, computer files and electronic communication systems including, in particular, email, telephone systems (fixed and mobile), texting, voicemail, MHA’s intranet and the internet. It refers to equipment and systems currently in place and those that may be acquired in future.
   2. Legal acts that govern the use of computer and telecommunication equipment include:
   * Copyright, Design and Patents Act, 1998
   * Computer Misuse Act, 1990
   * GDPR, 2018
   * Human Rights Act, 1998
   * Privacy and Electronic Communications (EC Directive) Regulations, 2003
   * Regulation of Investigatory Powers Act, 2000
   * Lawful Business Practice Regulations, 2000
   * MHA will also comply with other applicable legislation as required.
   1. Users may request assistance from the IT Service Desk - [ITServicedesk@mha.org.uk](mailto:itHelpdesk@mha.org.uk) in implementing this policy.
2. Scope and Purpose
   1. This policy is relevant for all computer users which includes MHA and subsidiary company colleagues, temporary workers, agency workers, volunteers, contractors, and anyone else engaging with MHA where:
   2. Computer equipment is accessed on or from MHA’s premises and accessed using MHA’s computer equipment or via access methods paid for by MHA.
   3. Personal equipment is used in a manner that identifies the individual with MHA or that references MHA in any manner.
   4. The purpose of this policy is to detail MHA principles and applicable standard operating procedures relating to computer usage at MHA including:
   * Acceptable Use
   * Passwords
   * End User Device Security
   * Anti-Virus and Anti Malware
   * Wi Fi usage
   * File Management and Storage
   * Exception Policy and Requests
   * Approved Software
   * Mobile Devices and Tablets
3. Definitions

| **Term** | **Definition** |
| --- | --- |
| **Users and End-Users** | All MHA colleagues including temporary workers, agency worker, and volunteers and any contractor, consultant, vendor, or colleague of a subsidiary company that is provided an MHA IT network account (Account). |
| **MHA Network** | Any wired or wireless network owned and / or managed by the MHA IT department. |
| **Computers** | Includes servers, thin clients, virtual desktops, desktop computers, laptops, tablets and mobile phones computer networks, software programs, computer files and electronic communication systems including, in particular, e-mail, telephone systems (fixed, mobile and SIP), texting, voicemail, intranet and Internet. It refers to equipment and systems currently in place and those that may be acquired in future. |
| **Personal Computer Equipment** | Includes thin clients, desktop computers, laptops, tablets, and mobile phones. It refers to equipment and systems currently in place and those that may be acquired in future. |
| **Computer viruses and malware** | Malicious computer programs or code designed to disrupt or disable computer equipment or steal information from the computer or network. |
| **Software** | Includes operating systems, desktop applications, business applications, tablets, and mobile phones apps. It refers to applications and systems currently in place and those that may be acquired in future. |
| **Approved Products** | These are the preferred products to use for the listed function. |
| **Tolerated Products** | These products should be avoided but may be used in limited circumstanced where approved products are not available or suitable. |
| **Prohibited Products** | These products must not be used under any circumstances for the function listed without a documented IT exception. |

1. Acceptable IT Usage
   1. Acceptable IT usage sets out the way in which information technology and electronic communications systems and internet access available MHA must and must not be used.
   2. This prevents colleagues from putting MHA or themselves at risk of prosecution for breaking one or more of the laws around computer use, data protection, communications, and human rights etc.
   3. Inappropriate use of MHA IT services puts MHA at risk of:
   * Data loss or compromise including breach of legal obligations to keep data secure.
   * Legal action against MHA or colleagues.
   * Unplanned downtime or unavailability of computer equipment which affects the ability of MHA colleagues to do their job effectively.
   * Financial loss due to inefficient use of technology.
   1. **Personal Usage**
      1. MHA computer resources may be used for personal purposes providing that:
   * the usage is primarily during non-working time (for example lunch breaks) and does not impact the users job role or completion of expected tasks.
   * excessive bandwidth is not used - for example by music or video streaming, which may impact the business operations of MHA.
   * MHA email addresses are not used to register or access non-business web sites and services
   * print volumes are minimised, and bulk printing is not carried out. Examples of bulk printing would include printing multiple copies of a non-MHA newsletter or brochure.
   * the usage is not prohibited as section 4.5 below.
   * The usage is for the colleague’s personal use only. Colleague’s must not provide MHA IT resources for use by non-colleagues such as friends and family. In particular Smartphones must not be used to replace home Wi-Fi as this can lead to extremely high data charges.
     1. Users may be responsible for excess charges identified as personal use.
     2. To ensure the security, integrity and availability of MHA systems, MHA provide hardware and software must be used to conduct MHA business whenever possible.
     3. The use of personal and home equipment not owned and managed by MHA is only permitted for the following uses:
   * Accessing MHA email through the “Outlook Web Access” facility. Users may open and view attachments but must not download attachments or save message to their personal computers.
   * Accessing MHA systems through the Azure Virtual Desktop / Remote Access service. This facility provides access to an MHA computer through a window on a personally owned computer.
   * Accessing MHA email, calendar, applications, and data on personally owned mobile phones or tablets that are registered with IT as users of the W5A Bring Your Own Device Smartphone service and have the relevant MDM (Mobile Device Management) software installed, to be reviewed and updated by the Associate Director of IT. Configuration of other devices to access MHA email is not permitted.
   * Access to each of the facilities above is granted on a case-by-case basis where there is business justification and may be revoked at any time.
     1. Note: documents must not be created or edited on personally owned devices. In particular Microsoft’s licence terms do not permit the “Home & Office” versions of Microsoft Office to be used for commercial use and copies run on personally owned devices may not be updated with the latest security patches.
   1. **Prohibited Usage**
      1. When using MHA IT services, activities that are strictly prohibited include, but are not limited to:
   * conduct of a non-MHA business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.
   * deliberate pointing or hyper-linking of company web sites to other internet sites whose content may be inconsistent with, or in violation of, the aims or policies of the company.
   * any conduct that would constitute or encourage a criminal offence, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US / UK export control laws and regulations.
   * use, storage, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or MHA.
   * transmission or storage of any proprietary, confidential, or otherwise sensitive information without the proper controls.
   * creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
   * any form of gambling.
   * export of MHA Assets (taking information out of the business).
   * unauthorised downloading of any software programs or files (see software allocation policy).
   * creating, uploading, or downloading material to / from unapproved websites which may bring MHA or its agents into disrepute.
   * generation or distribution of spam (unauthorised mass emails) or chain letters
     1. Users must:
   * **not** attempt to ‘hack’ into systems that they are not authorised to use.
   * **not** attempt to ‘crack’ passwords or use passwords that they are not authorised to use.
   * only log onto to MHA systems with either their own personal log-on, or a shared log-on they are authorised to use. Under no circumstances must another colleague’s personal log-on be used.
   * If any user believe they have access to unauthorised systems, software, or data they must report it to the IT Service Desk immediately.
   1. **Privacy Expectations**
      1. Users’ activities are periodically monitored. MHA reserves the right to perform an audit to examine email, personal file directories, web access, and other information stored on company systems, at any time and without notice.
      2. Other information that may be collected:
   * Printer usage
   * Mobile phone usage
   * Location data relating but not limited to mobile phones, tablets, laptop computers
   * File activity
   * Usage activity, log in/out and password changes
   * CCTV – some sites may have CCTV for site security
   * Phone systems - call logging is recorded
   * Door access – some systems record door activity related to your personal identification card
   * Time and attendance related systems. This includes a sign in picture
   * HR systems for personnel files
   1. **Email Confidentiality**
      1. Email is not a confidential means of communication. The company cannot guarantee that electronic communications will be private.
      2. Electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others.
      3. Once an email is transmitted it may be altered.
      4. Deleting an email from an individual workstation will not eliminate it from the various systems across which it has been transmitted.
   2. **Copyright and Intellectual Property**
      1. Before considering using any third-party content including downloading and printing a webpage, saving an image, cutting, and pasting content, or copying it for any other purpose, users must attempt to locate a copyright and / or usage statement from the author or publisher associated with that page. This might be on the site's ‘terms of use,’ legal pages or viewed on another page via a link, or on the cover pages of a printed resource.
      2. These terms might grant specific rights to users to use the material for certain purposes. Users must bear in mind that the person who placed the material on the internet might not have had any right to do so in the first place and that the copying and re-distribution of the material could be an infringement itself.
      3. If use of any third-party content is not covered by the terms of the site or if there is no statement, then the ‘fair dealing’ exceptions may apply. Users will need to ensure that use is compliant with all ‘fair dealing’ tests before the material is used. Failing that, users have to seek the permission of the rights holder to use the material.
      4. If using an MHA owned or managed device or network to stream music, video, or live broadcast (television), the user is responsible for ensuring they have the rights to do so. Note: the user licence for most streaming services (for example Spotify, Apple Music, Netflix, Amazon Prime) prohibits public broadcast or commercial use and puts MHA at risk of legal action. For the avoidance of doubt this includes using Amazon Echo and similar devices in shared and ‘common’ facilities such as day rooms and similar settings.
2. Passwords
   1. MHA’s policy on passwords complies with the cyber-security standards required by external partners and regulatory bodies including but not limited to
   * [Cyber Essentials Plus](https://www.ncsc.gov.uk/cyberessentials/overview) (UK Government)
   * Data Security Protection Toolkit (DSPT) ([DCB0086](https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0086-data-security-and-protection-toolkit)) (NHS)
   * [DCB1596](https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb1596-secure-email) (for NHS email)
   * [General Data Protection Regulation](file:///\\MHA-VM-FS01\Shares\Central%20Support\IT%20Systems\Policies\Future%20Draft%20Policies\General%20Data%20Protection%20Regulation) (GDPR) (EU Law)
   1. All IT equipment that supports an access control mechanism based on user accounts and passwords or PINs must have the mechanism enabled.
   2. User accounts must have a password or PIN set.
   3. It is recommended that passwords contain at least twelve characters to reduce the chance of compromise by a brute-force password-cracking attack.
   4. Passwords must contain at least eight characters, and meet 3 of the 4 criteria below:
   * English lowercase letters (a-z)
   * English uppercase letter (A-Z)
   * at least one number (0, 1, 2 etc)
   * at least one special character – for example $, @, or #
   * Note: due to a technical limitation on one of our systems the £ symbol cannot be used
   1. IT services that do not permit passwords that meet these criteria must have an approved IT exemption.
   2. Passwords **must** **not** be words found in a dictionary, personal information that can be associated with the owner - e.g., birthdays, telephone numbers - or simple patterns, e.g., abc123.
   3. Passwords **must** **never** be reused, either on the same system or account or between accounts.
   4. For MHA’s recommended process on setting a password, please see the Guidance section of this policy.
   5. Users with multiple user accounts for different services or multiple computers must set a different password for each account. Users must not use the same passwords for MHA and non-MHA (personal) user accounts. This will limit the risk of multiple accounts being accessed should any one user account be compromised.
   6. All passwords must be treated as sensitive, confidential MHA information. Users must not:
   * reveal their own user account passwords to anyone including Elevated Users. Under certain exceptional circumstances IT colleagues may require access to your user account . Under these circumstances sharing of your password with the IT colleague is permitted. It is recommended that you change your password once the ongoing issue has been resolved.
   * use the "Remember Password" feature of any operating system or application.
   * use the password storage features of web browsers.
   * write down or store passwords in any location easily accessible to others.
   * store passwords in an unencrypted computer file - e.g., MS Word, MS Excel.
   * disable the PIN, password, or fingerprint recognition on any MHA device.
   * Some laptops may have an encrypted Hard drive for storing local data. The password for accessing this drive is issued to the laptop user. The laptop user must not divulge the password to another person or write it down.
   * If someone demands a password, refer him or her to this document or have them contact IT Service Desk (ITServiceDesk@mha.org.uk).
   1. IT equipment access control mechanisms will enforce the password length and complexity detailed in section 2.1 to ensure user compliance.
   2. In addition, IT equipment access control mechanisms will further limit the risk of password compromise by enabling the following features where available:
   3. **Password History Control:** The access control mechanism will prevent the re-use of a user’s passwords.
   4. **Account Lockout:** The access control mechanism will prevent any further logins after five failed login attempts. The lockout will be for a fixed period of time or until the account is reset.
   5. **Concurrent Connections:** The access control mechanism will prevent an excessive number of concurrent connections by the same user above and beyond those reasonably required to access authorised and necessary Information Systems.
   6. **Grace Logins:** The access control mechanism will allow the user seven login opportunities to change their password when the password age limit is reached after which the account will be locked.
   7. **Smart Phones & Tablet Devices**
      1. All MHA issued smart phones & tablets configured must be protected by one of the following methods:
   * Fingerprint recognition/FaceID (with PIN code or password as a secondary option)
   * Password
   * PIN code only
   1. **Password Storage**
      1. Most users will have more users accounts with different passwords that can reasonably be remembered so will need a method of securing passwords. Acceptable password storage methods:
   * An approved password manager that stores passwords in an encrypted file – e.g., Keypass.
   * A MS Word or MS Excel document that is encrypted and password protected with a password that complies with this policy and is memorised (not written down)
   * A paper-based list that is not easily accessible to others – e.g., kept locked in a safe, drawer or similar where only the password holder has access.
     1. Passwords must not be stored using the following methods:
   * Web-based password managers – e.g., LastPass.
   * Password storage facilities on web browsers or browser plug-in-based password managers.
   * Plain text files and unencrypted documents.
   1. **Shared Passwords**
      1. For generic user accounts - those allocated to a role or site, used by multiple users - there is a requirement to share the password. Line or site managers must:
   * make sure only colleagues who need it have access to the password.
   * keep a record of who has the password at any given time.
   * the password is changed when anyone who knows it leaves MHA or job role.
3. End User Device Security
   1. This section establishes the minimum standards for the configuration and security of computer devices used by MHA colleagues.
   2. Users of MHA devices have a responsibility to keep the device, and the data and intellectual property that resides on it secure. Physical loss or compromise of a device can cause a significant financial loss to MHA through:
   * The cost of replacing the device
   * Any fines and reputational damage if data loss causes a regulatory breach
   1. Users should be aware that mobile computers are at greater risk of exposure to security threats than fixed location computer equipment permanently connected to the MHA network. The reasons for this include -
   * Maintaining the physical security of a mobile computer in-transit or at an off-site location may be more difficult.
   * Theft or loss of mobile computers is more likely, increasing the risk of unauthorised access to data stored on them.
   * Mobile computers may be connected to home or third-party networks that are less secure than the MHA network leading to higher risk of exposure to malicious attack.
   1. MHA does not require colleagues to store confidential information using computing devices that it does not own or manage. If this is required for a colleague’s job role a suitably configured MHA owned device will be provided according to the Hardware Procurement & Allocation Policy.
   2. All end user computer and mobile phones devices must be allocated to a designated person who is responsible for the security of the device. This may be a user (in the case of individually allocated devices) or a locally based manager (in the case of site-based devices).
   3. **User Obligations – All Devices**
      1. Any user of mobile devices or single-user computer equipment must:
   * inform the IT Service Desk (ITServiceDesk@mha.org.uk) of any known or suspected security-related problem with the computer equipment.
   * keep up to date with security announcements made by the IT Department and act on any instructions received.
   * allow software updates to be applied to their devices as issued by the MHA IT department and not to unreasonably delay or postpone those updates.
   * not install additional software as per the Software Allocation Policy.
   1. **User Obligations - Mobile Devices**
      1. Any user of mobile devices must:
   * use the device in a secure area. When using a mobile in public areas (cafes, trains, hotel lobbies etc) then users:

* must make sure the screen is not visible by others to protect MHA confidential information
* must not leave the device unattended. If you need to leave your seat (for example to go to the counter in a café) then take the device with you.
* must be aware of the possibility of opportunistic theft by snatching.
  + make sure that when the device is not with you, it is in a locked cupboard or drawer or attached by a secure cable lock to a fixed object.
  + make sure laptops are kept locked in the boot whilst travelling by car and take the device with you if you leave your car parked. Failure to do this could invalidate MHA’s insurance cover and may make the user liable to repay the cost of replacement.
  + avoid using Smartphones and other mobile devices on the street or other busy public areas that will put the user at risk of mugging or robbery. In particular be aware of standing where you may be in reach of thieves on cycles, mopeds or motorbikes looking to snatch devices.
  + make sure mobile devices are only used by MHA colleagues. MHA supplied devices such as smartphones and laptops must not be used by family members, residents, and suppliers due to risk of:
* non-MHA colleagues accessing confidential data on the device
* introduction of Malware or Viruses by users not aware of the MHA Anti-virus policy
* installation of unauthorised software
* configuration changes that may reduce the functionality of the device
  + use an access control mechanism (password, PIN number) as defined by the password policy. Where possible these may be implemented through administrative policies.
  1. **User Obligations - Portable Media**
     1. Any user of portable media (such as CD / DVDs, USB memory sticks, USB attached hard drives) must make sure:
  + All files on the device (regardless of content) are encrypted with the password set and managed in accordance with the Password Policy. Compliant approaches are:
* encrypting the whole device using hardware or software encryption
* encrypting each file individually (for example using the built-in feature of MS Word, MS Excel etc.)
* combining all the files on the device into a single encrypted zip file.
  + the device is kept physically secure at all times. When not in use or about the owner’s person, it should be kept securely locked away.
  + the device is not labelled with a description of the contents or the password.
  + Note: that USB sticks must not be used as the primary or only storage method for MHA data. Their intended use is the temporary transportation of data or files for use on another device. Data stored on USB attached devices is not backed up by the MHA IT department.
  + For USB attached hard drives used as permanent storage (for example Music Therapist kits), upon request the MHA IT department will keep a copy of the decryption key so that the data can be retrieved if the password is lost. This can only be done for a new hard drive or a used one that is completely wiped. Colleagues must contact the IT Service Desk for this to be done.
  1. **User Obligations - Theft or Attempted Theft**
     1. Actual theft or loss of hardware and software must be reported immediately on discovery, or as soon as is reasonably practicable, to the police and the IT Service Desk Manager or Associate Director of IT who will notify the MHA’s insurers.
     2. The Police incident number must be recorded and kept, as this may be required for insurance purposes.
     3. Attempted theft of IT equipment must be reported to the Associate Director of IT.
     4. Details of any personal data or sensitive personal data stored on stolen or lost equipment must be reported as soon as is reasonably practicable to the Data Protection Officer, so that appropriate action can be taken to assess the loss and if required report to the relevant authorities.

1. Anti-Virus and Anti Malware
   1. All computer equipment identified by the scope of the policy must have anti-virus software installed and operational. For MHA owned computer equipment, MHA will supply the anti-virus software, licence, and configuration to comply with this policy. Colleagues must not use any additional products not supplied by MHA as running multiple anti-virus products on the same computer equipment can produce inaccurate results.
   2. Any systems or computer equipment that cannot be configured with anti-virus software must be logged as an IT exemption.
   3. On first installation of the anti-virus software, a full virus scan of all attached storage devices (hard disks) must be completed.
   4. For workstations, personal computers, and laptops, if the anti-virus software provides an ‘always on’ background process to automatically scan files being processed by that computer, this must be turned on.
   5. Where the anti-virus software provides an automatic, scheduled virus scanning capability, this must be turned on. For computer equipment with ‘always on’ virus scanning, full virus scans must take place at least once a month. For computer equipment without ‘always on’ virus scanning, full virus scans must take place at least once a week.
   6. Suspicious files received via email, network download, disk, USB, or other media from unknown or untrusted sources must be scanned for viruses before being opened.
   7. If a user suspects their computer equipment has been infected by a virus or malware, they must run a full system scan immediately (contact IT for assistance).
   8. **Updating Virus Signatures**
      1. Virus signature files must be updated regularly. Where the anti-virus software provides automatic checking for new virus signatures, this must be turned on.
      2. For computer equipment with automatic checking, the software check for new virus signatures must take place at least once a day. For computer equipment without automatic checking, manual checks must take place at least once a week.
   9. **Disinfecting Computers**
      1. Once a virus is detected the infected files / system must be disconnected, disinfected, deleted and / or quarantined (contact IT for assistance). If the file cannot be disinfected or removed automatically by the anti-virus software, the user must inform the IT Service Desk as soon as possible.
   10. **Creation or Distribution of Viruses**
       1. Any activities undertaken with the intention of creating and / or distributing viruses or other malicious code are prohibited, in accordance with the MHA Code of Conduct.
2. Wi Fi
   1. MHA has two Wi-Fi networks:
   * METHODIST – this is a business only network used by MHA provided equipment and systems. Access is configured by the MHA IT department.
   * MHA-Guest – this is for free internet access for colleagues’ personal devices, people using our services (residents, scheme users) and visitors
   1. Users must not attempt to connect unauthorised equipment to the METHODIST Wi-Fi network.
   2. MHA-Guest Wi-Fi is available to colleagues, people using our services, guests, or visitors at MHA.
   3. Other wireless networks may be provided for specialist use and must not be used unless instructed to do so by the IT Department
   4. MHA reserves the right to exercise control over all activities on its IT facilities and networks, including monitoring of systems and electronic communications and access to external electronic resources to the extent permitted by the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. This Acceptable Use Policy constitutes formal notice that communications may be intercepted for reasons allowed within these Acts.
   5. To ensure effective running of MHA’s IT services, or to manage costs, MHA from time to time may impose controls on the use of systems including throttling bandwidth or capping download sizes or volumes. You must not attempt to circumvent such controls.
   6. **Using MHA’s Wi-Fi Connections**
      1. MHA-Guest is provided for: web browsing, email, video / audio conferencing, music & video streaming for non-commercial (personal) use.
      2. MHA provides no warranty with the use of MHA-Guest Wi-Fi. Users must take appropriate precautions to protect their computer and data.
      3. Guest devices must have an up-to-date anti-virus utility installed and active. Computers provided by MHA have this as standard.
      4. You must comply with all relevant external guidelines and law which affect your use of MHA’s networks, including (but not limited to) the Computer Misuse Act 1990, and GDPR 2018.
      5. **You must not:**
   * use MHA’s networks to engage in any unlawful activity, or to infringe MHA policies.
   * deliberately or recklessly act in a way which directly or indirectly causes disruption to others’ use of MHA’s networks or attempt to disrupt the use of IT facilities elsewhere.
   * knowingly download, transmit, store, generate or use any program, tool or virus designed to damage or disrupt or in any other way interfere with the IT facilities, and you must take sufficient care to minimise the risk of doing this inadvertently. If you suspect you have a virus, then you must take action to eliminate it.
   * use the Wi-Fi network in to create, transmit, store, download or display images, data or other material that may be deemed offensive, obscene, indecent, or menacing.
   * use MHA’s networks to defame, harass, offend, or hinder another person, by creation, transmission, storage, download or display of materials, or by other means
   * send an email or message that does not correctly identify you as the sender, or which appears to originate from another person, or otherwise attempt to impersonate another person. You must not send unsolicited emails to a large number of recipients.
   * use the networks to create, access, store or transmit material in a way which infringes a copyright, trademark, or other intellectual property right.
3. File Management and Storage
   1. All files access (create, edit, open, and delete) on the network and intranet may be recorded, may be used for analysis, and may be reported if the access is deemed in breach of this or other policies.
   2. All files stored on the network, the intranet, laptops, tablets, and smart phones remain the property of MHA.
   3. Personal files may be stored as long as it does not breach this or other MHA policies. Files of this type may be deleted without notice to protect MHA. To deem data as personal it must be stored in a folder called ‘Personal.’
   4. MHA reserves the right to access all files held on MHA’s computer equipment or equipment used on behalf of the MHA.
   5. Note: Computer Equipment: includes thin clients, virtual desktops, desktop computers, laptops, tablets and mobile phones computer networks, software programs, computer files and electronic communication systems including, in particular, e-mail, telephone systems (fixed and mobile), texting, voicemail, intranet and Internet. It refers to equipment and systems currently in place and those that may be acquired in future; or any other IT items that are easily moved.
   6. **Prohibited File Types**
      1. Data storage is a finite resource that has a cost to MHA. The following file types must not be stored on MHA computer equipment or services:
   * Video, music, or any other media where MHA is not the copyright owner or does hold a licence to store and use the copyrighted material
   * Video, music, or any other media files not for business use
   * Software installation files and source code unless stored by the MHA IT department in an approved location
   1. **Permitted Storage Locations**
      1. Users must only store files in permitted storage locations. This ensures that the files are kept available (through backups) in the event of an IT failure, the files are kept secure (access is controlled) and MHA can comply with relevant data protection legislation.
      2. Note: Users means all MHA colleagues, temporary workers, agency colleague, and volunteers and any contractor, consultant, vendor, or colleague of a subsidiary company that is provided an IT network account - Account).
      3. Files must be stored on MHA network drives (usually access through a drive letter on a user device) or MHA supplied tablets or Smartphones. Files must only be stored on Windows desktop on a temporary basis and users should be aware that they may be deleted at any time.
      4. Files may be stored temporarily on portable storage media (external hard drives, USB sticks etc.) for the transportation or transfer providing the files are a copy of files retained on an MHA network drive, the storage is secure (encrypted) and temporary.
      5. Files must not be stored on non-approved cloud-based services (such as Dropbox, Google Drive etc). Only the MHA provided instance of Microsoft OneDrive is permitted. Any other version of OneDrive is not authorised.
   2. **Access Control**
      1. File access will be managed on the information security principle of “least privilege” (or “least authority,” which states that each user must only be able to access the information or resources necessary for their job (role-based access control).
      2. Access will be managed by the MHA IT department. The role of access management is to make sure that individuals in an MHA are able to use the MHA operating systems, network services and application software to help them do their job, and only have as much access to them as they really need.
      3. Users are responsible for informing the MHA IT department (via the IT Service Desk) when new files or folders need access restricting to individuals, roles, or departments or when existing access needs changing.
4. IT Exception Policy and Procedure
   1. IT policies and standards are in place for the benefit of MHA to ensure IT services provided to colleagues and customers are safe, secure, dependable, and cost efficient. However, it is recognised that there may be situations where it is more pragmatic or responsive to vary a policy. Any exception to a policy or standard must be carefully impacted to assess the cost vs benefit of not following policy or standard.
   2. The IT exemption policy must be used where another IT policy or standard states that an exemption is possible. Currently this includes (but is not limited to):

| Policy / Policy Section | Exemption |
| --- | --- |
| Hardware Procurement and Allocation | Purchase and use of hardware not on the approved hardware list |
| Hardware Procurement and Allocation | Personally allocated devices outside of policy |
| Hardware Procurement and Allocation | Purchase of hardware scheduled to be out of manufacturer support within the minimum refresh cycle |
| Passwords | IT systems that do not allow the password criteria defined by the policy to be to be set and enforced |
| Anti-Virus | IT systems that do not allow Anti-Virus software to be installed and / or configured |
| Architectural Standards | New systems or changes to existing systems that do not comply with MHA architectural standards. |
| Other | To be used for an ad-hoc exemption not specifically described by a policy |

* 1. The Associate Director IT can request the exemption policy is used at any time for IT policies and standards not listed.
  2. The following process must be used to request and approve an exemption:
  + The requestor completes an exemption form in Appendix 1 and submit completed form to the IT Service Desk.
  + The IT Service Desk will mark the ticket as a “Request for Change” and allocate to the Management team queue.
  + The request will be reviewed within five working days, which may include consultation with the requestor.
  + A decision will be made and recorded. The request ticket will be updated with the decision and the requestor informed.
  1. Any MHA colleague can raise an exemption request.
  2. Exemptions can only be approved by the Associate Director IT or their nominated deputy.
  3. All exemptions will be recorded in a document held by and available to the MHA IT department. As a minimum the document will record:
  + The policy or standard the exemption applies to
  + A description of the exemption or variation to the policy
  + The rationale for requesting the exemption
  + Who requested the exemption
  + Who reviewed the exemption (may be more than one person)
  + The request decision
  + Any conditions (e.g., time period, regular review)

1. Approved Software
   1. Computer software is selected, deployed, and funded by MHA IT who carefully evaluate the best software to meet MHA’s business needs balancing cost, security, supportability, and ease of use.
   2. Although IT control the availability of most software packages there are exceptions such as:
   * Software that is built into operating systems (such as Windows or Android) and cannot be removed
   * Software that IT provide on Smartphones and tablets for personal use (only) as a courtesy to colleagues who wish to use their MHA mobile phone for reasonable personal use
   1. Some software is only licenced for personal or home use, or in certain situations. Using incorrectly licenced software can put MHA at risk of legal action and significant fines as well as loss of NHS and Local Government contracts.
   2. All software used in MHA is assessed for information and cyber-security to ensure we meet our legal and regulatory obligations for keeping data secure. Software from unapproved sources may be counterfeit or contain hidden malware or viruses
   3. There are situations (such as investigations) where the use of software and the content it generates needs to be logged / archived and reportable. Approved MHA software allows compliance reporting where needed
   4. All computer software or systems to be used by MHA must be acquired through the IT Department and normally funded from the IT budget. Individual departments are not permitted to use their budgets to fund IT or system development with approval from the Hed of IT and Finance Director.
   5. All computer software must be purchased new from approved suppliers and compliant with MHA procurement policies.
   6. To minimise the cost of IT services, the MHA IT department at its discretion, will reuse and redistribute or reallocate licensed applications between colleagues or computers.
   7. Where specific job-related applications are required, requests should be submitted through IT Service Desk. These requests will be assessed and dependant on license availability the application will be allocated.
   8. For a list of approved applications, see Appendix 2.
2. Roles and Responsibilities

| Role | Responsibilities |
| --- | --- |
| **All Users** | * All users must follow the corporate principles regarding resource usage and exercise good judgment in using the internet. If you have any questions, please contact the MHA IT Department. * Users of MHA devices have a responsibility to keep the device, and the data and intellectual property that resides on it secure. * Making sure that anti-virus software is installed and operating on all MHA workstations, personal computers, or laptops they have been personally allocated and any non-MHA devices they attach to any MHA network. * Making sure that any third parties or guests, only connect to the MHA Free Wi-Fi and are aware of this policy and comply with it. |
| **Line Management** | * Line managers are responsible for making sure that this policy is applied within their area. They must discuss any queries they have on the application or interpretation of this policy with the IT Department prior to any action being taken. |
| **IT Department** | * When authorised to do so, complete compliance audits relating to acceptable usage of IT equipment. * Responsible for making sure that anti-virus software is installed and operating on all MHA owned, managed servers and shared computer equipment. |
| **Associate Director of IT** | * Overall Responsibility for all IT Services within MHA |
| **Data Protection Officer** | * Where necessary, to authorise compliance audits relating to acceptable usage of IT equipment. |
| **Director of People and Communications** | * Where necessary, to authorise compliance audits relating to acceptable usage of IT equipment. |
| **Associate Director of IT and Director of Finance** | * Where necessary, to authorise compliance audits relating to acceptable usage of IT equipment. * To authorise external audits relating to the acceptable usage of IT equipment if necessary. |

1. Training and Monitoring
   1. Compliance is assessed through direct observation, monitoring, and supervision of our colleagues.
   2. Audits relating to the acceptable usage of IT may take place to ensure computers users are compliant with legal regulations, MHA’s policies, and procedures, and for purposes of company information system management. Auditors may also be procured externally (authorised by the Director of Finance and IT), Auditors may request and shall expect assistance from administrators or users responsible for the IT equipment being audited.
   3. Where a normal audit uncovers a potential criminal matter or adult / child pornography, the audit must be stopped immediately, the IT equipment quarantined to a secure location and the Associate Director of IT notified.
2. Communication and Dissemination
   1. This policy is disseminated and implemented within all MHA services through MHA’s channels of communication.
   2. Each colleague’s line manager must ensure that all teams are aware of their roles, responsibilities.
   3. This policy will be available to the people we support and their representatives in alternate formats, as required.
   4. Any review of this policy will include consultation with our colleagues, review of support planning, incident reports, quality audits and feedback from other agencies.
   5. Queries and issues relating to this policy should be referred to the Standards and Policy Team [policies@mha.org.uk](mailto:policies@mha.org.uk)
3. EDI Impact Assessments
   1. Equality, Diversity, and Impact Assessment to be confirmed.
4. Resources
   1. MHA policy documents, procedures, and guidance:
   * [HR8.3: Code of Conduct Policy](https://intranet.mha.org.uk/Interact/Pages/Content/Document.aspx?id=2486&utm_source=interact&utm_medium=quick_search&utm_term=code+)
5. Appendices
   * Appendix 1 - Exception Request Form
   * Appendix 2 – Approved Applications List

Appendix 1: Exception Request Form

|  |  |
| --- | --- |
| **Requester Name** |  |
| **Requester Email** |  |
| **Exception Type** | e.g., Other (see table in Exception Section) |

|  | **Request Details** | **Answer** |
| --- | --- | --- |
| 1 | Please describe the exemption being applied for. What is being requested different from the policy? |  |
| 2 | Please describe the rationale (why the exemption is needed) and why the policy cannot be applied |  |
| 3 | Please describe the impact on MHA if this exemption is not granted including any additional cost or risk incurred |  |
| 4 | Is this a permanent exemption or temporary? If temporary, please provide your planned timescale |  |
| 5 | Please provide any other information that supports the request |  |
| **Requester Signature** | |  |
| **Date of Request** | |  |
| **Request Approved by (include job title)** | |  |
| **Approval Date** | |  |

Appendix 2: Approved Applications List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Function | Approved Product(s) | Tolerated Product(s) | Prohibited Product(s) | Notes |
| **Ai Notetaker** | Otter.ai (MHA Instance only & Limited Licences) | None | All Others |  |
| **Anti-Virus** | Checkpoint Clam (T&A Terminal) | None | All Others |  |
| **CAD Viewer** | DWG TruView | None | All Others |  |
| **Cloud Storage** | Microsoft OneDrive (MHA Instance only) | Google Drive Dropbox Microsoft OneDrive | All Others |  |
| **Diagramming/Workflow** | Microsoft Visio (Limited Licenses) Microsoft PowerPoint | Archi | All Others |  |
| **Email Client** | Microsoft Outlook | None | All Others |  |
| **File Archiver** | 7-Zip | None | All Others |  |
| **Instant Messaging** | Microsoft Teams | IM function of Facebook Workplace for conversations that do not record business decisions or data | WhatsApp All Other Instant Messaging Apps | WhatsApp is provided on MHA Smartphones for personal use only. |
| **Internet Browser (Windows based devices)** | Mozilla Firefox Microsoft Edge Google Chrome | None | All Others |  |
| **Internet Browser (Android / iOS devices)** | Soti Surf | Chrome (Android/IOS)  Safari (iOS) | All Others |  |
| **PDF Editor** | Nitro PDF (Limited Licenses) Microsoft Word (Limited Functionality) | None | All Others |  |
| **PDF Reader** | Adobe Acrobat DC Reader Internet Browser in Built | None | All Others |  |
| **Photo Editor** | Adobe Photoshop (Limited Licenses) | Gimp Adobe Photoshop Express / Elements Built-In Windows Apps | All Others |  |
| **Presentation** | Microsoft PowerPoint | None | All Others |  |
| **Project / Task Management** | Microsoft Project (Limited Licenses) | Freedcamp | All Others |  |
| **Publishing** | Microsoft Publisher | None | All Others |  |
| **Remote Access** | Teamviewer | UltraVNC provided by IT Dept | All Others |  |
| **Spreadsheet** | Microsoft Excel | All Others | All Others |  |
| **Database** | Microsoft SQL\*Server | None | All Others |  |
| **Audio / Video Conferencing (Hosting)** | Microsoft Teams | Zoom | Powwownow (audio)  Skype (consumer version) |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Function | Approved Product(s) | Tolerated Product(s) | Prohibited Product(s) | Notes |
| **Audio / Video Conferencing (Participant)** | Microsoft Teams | Host Solution | N/A | MHA colleagues invited to meetings by external contacts may use the product the host has chosen |
| **Video Editing** | Adobe Premiere (Limited Licenses) Windows InBuilt Apps | None | All Others |  |
| **Video Player** | VLC Player Windows InBuilt Apps | Internet Browser in Built | All Others |  |
| **Word Processing** | Microsoft Word | None | All Others |  |
| **Business Intelligence / Management Reporting** | PowerBI | Business Objects  Crystal Reports  Qlikview | All Others |  |
| **HR** | iTrent | None | All Others |  |
| **Finance** | Open Accounts |  | All Others |  |
| **Workflow** | eBis | None | All Others |  |
| **Fundraising** | Raisers Edge | None | All Others |  |
| **Care Home Income Processing** | CareSys | None | All Others |  |
| **Document Management** | Filestream | None | All Others |  |
| **File Storage** | Shared Drives (Microsoft File Server)  Sharepoint  Microsoft One Drive (MHA Instance only) | Intranet  Google Drive Dropbox Microsoft OneDrive  Microsoft SharePoint | All Others | Music Therapists may store video / audio files on the portable hard disks issued by IT. |
| **Screen Capture (for creating training)** | Camtasia | None | All Others |  |
| **Speech Recognition** | Dragon Professional Individual | None | All Others | Must be accompanied by a RI Assessment Form |
| **Request Management** | 4Me | None | All Others |  |

1. Version Control

| Version | Version Date | Revision Description / Summary of Changes | Author and Review Panel | Next Review Date |
| --- | --- | --- | --- | --- |
| 1 | October 2023 | * Policy developed as an amalgamation of existing computer use related policies (each section of this policy). * Policy reviewed in line with compliance review due date. | Head of IT  Standards and Policy Manager | October 2025 |
| 2 | April 2024 | * Approved file storage Microsoft One Drive (MHA Instance only) | Head of IT  Standards and Policy Manager | October 2025 |
| 3 | April 2025 | * Approved AI Notetaker Otter.ai (MHA Instance only & Limited Licences) Appendix 2 * Change of Job Title from Head of IT to Associate Director of IT | Associate Director of IT  Head of Standards and Policy | October 2025 |