Information Technology Policy and Procedures

Responsible Person	IT Manager
Author	IT Manager
Date Effective From	Mar-15-2018
Date Last Amended	02-01-2024
Reviewed By	

1. Table of Contents

1 Introduction and policy statement

1.1 This document sets out the Information Technology (IT) Policy for MHCPL for the protection of its IT systems and defining baseline responsibilities for security, equipment and file storage. “IT systems” refers to the MHCPL IT network, hardware including portable media, system and application software, communication components including telephone and WAN systems, documentation, physical environment and other information assets. It does not include IT systems not connected to the MHCPL IT network.

1.2 This Policy covers the IT networks for MHCPL staff across all sites and the separate network provided for Evidence & Practice Information Management and Technology.

1.3 The equipment covered by this policy includes:

- Network Infrastructure – The equipment housed internally to provide the MHCPL IT network, including servers, enclosures, racks, cabling, switches/hubs, Routers, wireless access points, firewalls, proxies, authentication systems, devices and remote access systems.
- Desktops – Personal Computers (PCs) issued or provided to staff in the course of carrying out their duties. Mouse and keyboard are provided along with Desktops to carry out the business functions. DGM and above will get wireless mouse and wired keyboard. Other Employee should seek approval from their HOD with business justification to receive wireless mouse.
- Laptops/Netbooks -Portable Personal Computers issued or provided to staff in the course of carrying out their duties. Mouse and keyboard are provided along with laptops to carry out the business functions. AGM and above will get wireless mouse and wired keyboard. Other Employee should seek approval from their HOD with business justification to receive wireless mouse.
- Mobile Phones – Digital communication devices issued or provided to staff in the course of carrying out their duties will be maintained by HR team. Email will be configured for GM and above, other employee should seek approval with business justification.
- Desk Phones – Telephones/Voice Communication devices connected to the Network Infrastructure including desk telephones, analogue telephony adaptors, DECT telephones (cordless). By default, MHCPL employee need to share the analog desk phone to carry out the business functions.
- Media/Portable Media – Electronic Storage Devices such as DVDs, CDs, memory sticks and hard drives issued or provided to staff in the course of carrying out their duties.
- External Communications Infrastructure – Equipment used to connect MHCPL to the external world including the Wide Area Network, analogue telephone lines, digital telephone lines, leased lines and all related equipment and services.
- All related Facilities controlled IT media used in MHCPL’s meeting rooms.

1.4 The objective of this policy is to ensure: -

- the confidentiality of data and information assets are protected against unauthorised disclosure and incidents are promptly reported (see section 9)
- the integrity of data and information assets so that they are protected from unauthorised or accidental modification
- the availability and accessibility of IT systems as and when required by staff.

1.5 This policy sets out the principles of IT security including the maintenance, storage and disposal of data and explains how they will be implemented at MHCPL to ensure there is a centralised and consistent approach to IT security.

1.6 One of the aims of the policy aims to raise awareness of the importance of IT security in the day to day business of MHCPL.

1.7 The policy supports the MHCPL business objectives of ensuring that the security, integrity and availability of IT systems are balanced against the need for staff to access systems and services that are necessary for their job, within the limits imposed by this policy. It will also help to protect data from misuse and to minimize the impact of service disruption by setting standards and procedures to manage and enforce appropriate IT security.

1.8 The policy supports the legal obligations of MHCPL to maintain the security and confidentially of its information, notably under the Data Protection and are the Information Technology Act, 2000.

2 Scope

2.1 This policy applies to all MHCPL IT systems and those working at or for MHCPL (Users):

- All MHCPL employees (including MHCPL staff on secondment to other organizations)
- Agency workers
- Contractors, where they are directly using MHC's network.
- Secondees (those who are seconded to MHCPL from other organizations) with authorised access to the IT network.

3 Responsibilities

3.1 Defining responsibilities ensures that all users of MHCPL IT systems are aware of their responsibilities to minimize the risks to IT security and operations.

3.2 The MHCPL Manager is responsible for ensuring that:

- electronic filing systems and documentation are well maintained for all critical job functions to ensure continuity.
- no unauthorised staff are allowed to access any MHCPL IT systems in any location, as such access could compromise data integrity.
- named individuals are given authority to administrate specific computer systems according to their job function and role following the principle of least privilege.
- robust disaster recovery and business continuity procedures to be in place.
- all current and new users are instructed in their security responsibilities.
- Procedures are implemented to minimize MHCPL's exposure to fraud, theft or disruption of its systems; these include segregation of duties, dual control and staff rotation in critical susceptible areas.

3.3 The MHCPL IT department has the following responsibilities:

- Day to day responsibility for the management and security of the systems, equipment and services laid out in section 1.3, with specific technical responsibilities being allocated across the team/s.
- To make all users aware of this policy and to ensure that users understand and are able to abide by them when carrying out work on MHCPL's behalf.
- Monitoring and reporting on the state of IT security within MHCPL and across all MHCPL systems.
- Developing and enforcing detailed procedures to maintain security access to all MHCPL systems.
- Ensuring compliance with relevant legislation, policies and good practice for all internal systems.
- Monitoring for actual or potential IT security breaches for all internal systems. And reporting to the appropriate people as need be.
- Maintaining an IT asset register (see section 5.1).
- The allocation/disposal/reallocation of all computer hardware and software to ensure best practice usage, value for money and that all data storage devices, including portable electronic media, are purged of sensitive data (such as confidential or personal information) before disposal or reallocation.
- Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence in accordance with the Incident Reporting procedure.
- Purchasing all computer equipment and software/license to ensure value for money, consistency and compliance. The IT assets(Desktop/Laptop/Printer/datacard) required to be purchased for the department should follow an approval process. (Refer SOP : MHCPL_IT-facilities_form).

3.4 MHCPL IT Manager of department has the following responsibilities:

- Day to day responsibility for the management and security of the Evidence and Practice IT Infrastructure and systems, along with any externally hosted or supplied systems and services. Specific technical responsibilities will be allocated across the IT Operations team.

- To ensure all Users and Systems comply with this policy and further directions that comply with this policy as issued by the IT Head from time to time.
- Monitoring and reporting on the state of IT security for which they are responsible.
- Providing information on a timely basis to the MHCPL IT team to maintain an Inventory Management system for MHCPL
- Ensuring compliance with relevant legislation.
- Monitoring for actual or potential IT security breaches within the MHCPL IT systems for which they are responsible. And reporting to the appropriate people as need be.
- Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence in accordance with the Incident Reporting procedure.
- Ensure any and all information as reasonably required by the Management is provided to fulfil its compliance roles.

3.5 The Human Resources department is responsible for ensuring that:

- all MHCPL staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment, and any contactors, temporary staff (including agency staff) and secondees sign MHCPL's standard confidentiality undertaking before they are permitted to use MHCPL systems.
- the MHCPL IT and Evidence and IT Head are both notified immediately via the Starters / Leavers / Changers process about changes to user permissions so that access to the IT network can be amended as appropriate. This may include any instance where a member of staff is temporarily suspended from their duties.
- new staff are given basic user training in IT Security as part of their induction.

3.6 Users who do not have administration rights over their issued equipment are responsible for ensuring that:

- No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote login data secure (except where necessary to disclose them to the IT department for administrative purposes) and to deny unauthorised third party access to MHCPL systems. This is particularly important for home workers and when using wireless networks.
- All reasonable care is taken to protect the security of IT equipment they are issued together with confidential data stored on it when taken outside secure offices.
- All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the MHCPL IT department regardless of the working state of the equipment.
- Contractors engaged by MHCPL are provide with and comply with this policy.
- Sensitive data stored on portable IT equipment is kept to the minimum required for business use and encrypted in order to minimize the risks and impacts should a security breach or loss of that equipment occur.
- Actual or suspected security breaches are reported as soon as they arise.

- Only staff explicitly authorized by the MHCPL IT dismantle, repair or alter MHCPL supplied equipment Further advice is contained in Appendix A.

3.7 Users who do have administration rights over their issued equipment are responsibility for ensuring that:

- No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote login data secure (except where necessary to disclose them to the MHCPL IT for administrative purposes) and to deny unauthorised third party access to MHCPL systems. This is particularly important for home workers and when using wireless networks.
- All reasonable care is taken to protect the security of IT equipment they are issued with together with confidential data stored on it when taken outside secure offices
- All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the MHCPL IT department regardless of the working state of the equipment.
- Contractors engaged by MHCPL are provide with and comply with this policy.
- Sensitive data stored on portable IT equipment is kept to the minimum required for business use and encrypted in order to minimize the risks and impacts should a security breach or loss of that equipment occur.
- Actual or suspected security breaches are reported as soon as they arise.
- Only licensed or in house developed software, specifically required for their job within MHCPL, is installed upon the equipment for which they are responsible
- The equipment for which they are responsible for is only used for work purposes (no private use) and specifically their own job.
- All due skill, care and attention is taken to ensure that no virus, Trojan spyware or other malware is introduced to their equipment or MHCPL systems
- All due skill, care and attention is taken to ensure that no configuration, miss-configuration or alteration to systems, software, equipment or infrastructure has a detrimental effect on the normal running, availability or stability of the MHCPL IT Infrastructure as detailed in section 1.3
- Only staff explicitly authorised by the IT Manager for Operations dismantle, repair or alter MHCPL supplied equipment. Further advice is contained in Appendix A.

4 Security

4.1 Technical security measures will be put in place to protect MHCPL systems from viruses and other malicious software, and all IT systems will be monitored for potential security breaches.

4.2 Email and internet use will be governed in accordance with the Email and Internet policy.

4.3 Allocation of accounts to temporary workers using a generic username that cannot be mapped back to the user will not be allowed.

4.4 All relevant contracts with third parties will include standard Office of Government Commerce clauses on information security. All central processing equipment, including file servers, will be covered by third party maintenance agreements.

4.5 All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the MHCPL IT department.

4.6 All IT equipment, including virtual systems, will be uniquely identified and recorded.

4.7 Environmental controls will be maintained in the server/communications rooms of all premises to protect key equipment. Smoking, drinking and eating is not permitted in these areas.

4.8 All MHCPL laptops must be encrypted with access to MHCPL IT networks and applications via using a strong authentication method(VPN).

4.9 Access to premise server/communications rooms will only be with the express permission of the MHCPL IT Department and accompanied by the appropriate representative.

4.10 CYBERCRIME STANDARDS: 9 Steps to Safeguard Your Organizations Data and Technology

There's a strong argument to be made that "Cybercrime" is more of a threat than a physical crime to most people and organizations. The more you think about the hypothesis, the more alarming it becomes.

A physical crime typically depends upon the victim and the perpetrator (or group of perpetrators) being in the same place at the same time. That requirement doesn't hold true for individual hackers, sophisticated crime syndicates, foreign governments, or corporate espionage specialists. Vast underground networks of digital criminals trade information and conspire for purpose of sabotage, theft, and fraud, often working across borders that place them out of reach of law enforcement.

For the past decade, security has consistently ranked as a top concern of CIOs. While other issues have come and gone, security has remained a vital issue because the capabilities and sophistication of cybercriminals have often outpaced the measures taken to protect against them. A layered approach to security has been consistently recommended, but the reality is that it is neither sufficient for an organization of any size to depend on antivirus, antispam, and a firewall. The ingenuity and persistence of today's criminals require much more than that.

IT department should follow the below recommendations as part of cybercrime :

1 Install a firewall and ensure that it is properly configured to ensure that no potential points of entry are left undefended.

2 Install and regularly update advanced antivirus protection. Not just for PCs, but for Macs and tablets as well.

3 Maintain advanced antispam protections. Email remains a key point of vulnerability for most organizations.

4 Implement web/internet filtering. In recent years, malicious websites have emerged as the most popular entry point for malware.

5 Ensure that systems promptly receive all official recommended updates for both system software and applications.

6 Implement comprehensive system monitoring to rapidly detect and isolate any hostile events.

7 Maintain comprehensive, frequent, reliable backup and recovery systems capable of meeting RTO(Recovery Time Objective) and RPO(Recovery Point Objective) objectives – a vital measure in the event that data is wiped or locked by malware.

8 Implement user education on security and safe use practices including "BYOD" (Bring Your Own Device) and company-issued tablets. Set security standards for user conduct, and enforce them.

9 Conducting audits with internal team to follow security practices for vulnerability at least once a year.

Maintaining effective security consumes resources, time and attention – but such expenses are minimal compared to the potentially catastrophic impact of a successful intrusion.

5 Software protection

5.1 Only licensed copies of commercial software or in house developed software Connectivity is the connection between MHCPL IT systems and the MHCPL intranet are used by MHC. The MHCPL IT department will maintain a register of all commercial software, including all software licenses, to ensure that MHCPL complies with license conditions and relevant law. Users must not install ANY externally developed software on MHCPL IT equipment without prior approval of the IT department.

5.2 All users are reminded it is a criminal offence to make or use unauthorised copies of commercial software and that offenders may be liable to disciplinary action.

5.3 Software products required by any department should be approved by the MHCPL IT Department prior to purchase. Unless otherwise directed all software purchasing and licensing will be carried out by the MHCPL Procurement department, and users must follow any instructions issued with regard to specific software or applications.

5.4 MHCPL will minimize the risks of computer viruses through education, good practice and procedures, and application of robust anti-virus software and ensuring firewall policies follow appropriate national guidelines. Users must report any detected or suspected viruses, Trojan, spyware or malware on their computers immediately to the MHCPL IT Department as appropriate.

6 Physical access controls

6.1 Physical access controls to secure areas will minimize the threat to the MHCPL IT systems through damage or interference. The MHCPL IT department will be responsible for access to all IT systems located in secure areas, with access being restricted using the principle of least privilege. An entry restriction system to the server/communications rooms at all premises will be implemented.

6.2 The server/communications rooms and store rooms for IT equipment will be locked at all times and the keys/codes held securely by the MHCPL IT department or the Security Team.

6.3 Authenticated representatives of third party support agencies or other parties will be given access through specific authorization from the IT Manager and will be supervised by MHCPL IT department representatives while on site.

6.4 No remote access to MHCPL IT systems will be given to third parties at any time unless specific authorization is received from IT Manager. Such access if granted must be supervised at all times.

7 User access control to the IT network drives

7.1 User access to the IT network drives will be granted where access is necessary to perform the person's job following the principle of least privilege. Access will be modified or removed as appropriate when a person changes job or leaves MHCPL. It will be the responsibility of the HR department to notify the MHCPL IT department immediately of any changes required to access controls, and procedures will be established between the three teams to ensure this happens.

7.2 For those with existing access to the IT network, requests to change access permissions should be made to IT. These will be authorised by IT Manager who will, if necessary, check the requirement with the relevant HOD.

7.3 No individual will be given access to the IT network unless properly trained and made aware of his or her security responsibilities.

7.4 Each member of staff will be provided with a minimum of 5% storage space on their 'E drive'. This storage space is free for the individual to use (subject to sections 7.5 & 7.6 below). If this storage limit is exceeded then the E drive will be unable to save any additional data – it is individual's responsibility to manage this allocation.

7.5 'E drives' remain part of the MHCPL IT systems and MHCPL has full rights of access to all data stored on its IT network. The content of E drives is not routinely monitored but MHCPL reserves the right to view content if there are reasonable grounds for doing so; for example to prevent fraud or suspected breach of MHCPL policies. Further information is contained in the Email and Internet policy.

7.6 Users are not permitted to store entertainment files (including but not limited to music, pictures, video, electronic games) upon the MHCPL IT systems. Files which have the same nature but are for work purposes must be notified to and approved via the MHCPL IT department.

8 Disposal/reallocation of equipment

8.1 Equipment allocated to an individual user (including memory sticks) must not under any circumstances be reallocated within a department (or any other user) and must always be returned to MHCPL IT for reallocation to ensure correct management of sensitive data

8.2 Where the equipment is deemed to be of no use to private individuals, it will be either disposed through Scrap sale.

9 Security incident investigation and reporting

9.1 The objective of security incident investigation is to identify detect, investigate and resolve any suspected or actual computer security breach.

9.2 A security incident is an event that may result in:

- degraded system integrity
- loss of system availability
- disclosure of confidential information
- disruption of activity
- financial loss
- legal action
- unauthorised access to applications
- loss of data

9.3 Incidents should be notified to the IT Team or the IT Manager of Operations (IT) as appropriate.

9.4 All users must report actual security breaches, or any concerns or suspicions about security breaches, as soon as they arise.

9.5 All actual security incidents will be formally logged, categorized by severity and actions recorded by the MHCPL IT department.

10 Disaster recovery and business continuity

10.1 All business critical data will be replicated between servers at relevant locations so that if the servers in one location become unavailable, access is automatically switched to the servers in another location.

10.2 All data will be backed up regularly to backup devices. Critical computer equipment must be fitted with battery back-ups (UPS) to ensure that it does not fail during switchovers or emergency shutdowns.

10.3 To minimize the risk to MHCPL IT systems, robust disaster recovery plans will be put in place to ensure:

- identification of critical computer systems.
- identification of areas of greatest vulnerability and prioritization of key users and user areas.
- agreement with users to identify disaster scenarios and what levels of disaster recovery are required.

11 Data Backup

11.1 System back up is taken on daily basis and it was scheduled to run every day using an application.

11.2 SAP server online back up was scheduled on run on daily basis at 4 AM IST and full back up(offline) was scheduled weekly. The backup was scheduled to write on to the tapes and they are stored at SERVER location. The logs are maintained for 30 days .

11.3 Disaster recovery is not implemented. Planned for the DR during our SAP Upgrade.

12 Risk management

12.1 The objective of risk management is to identify, counter and report on actual and possible threats to IT systems.

12.2 Significant IT risks will be included in the MHCPL risk register and will be made available to Management.

13 Auditors

13.1 The implementation of MHC's IT policy and procedures will be subject to periodic review.

13.2 The review should happen by both internal and external auditors and the subsequent recommendations will be agreed and action plans put in place and monitored.

14 Compliance

14.1 Breach of this policy may result in disciplinary action in accordance with the MHCPL Disciplinary Policy and Procedure.

14.2 Any breach of the law will be reported to the appropriate authorities.

15 Review

15.1 This policy will be monitored by the IT department to ensure it is fit for purpose and reviewed every 3 years or for any major changes.

2. Appendix A

Good Practice Guide

Below is a summary of recommended Do's and Don'ts for all users of MHCPL IT systems. It is intended to complement approved MHCPL policies and support new information governance standards.

- Do ensure you keep security in mind when working – If you have been sent a file or a web link, are you sure you can trust the person it came from, is this the type of thing they would normally send, does it 'feel right'? Remember, lots of spam and viruses sent impersonate the e-mail address of a real person, so the e-mail may not have been sent by the person you think. Lots of viruses move from machine to machine as hidden files on storage devices. Remember, only IT equipment issued, or approved, by the MHCPL IT department should be used, except where personal PCs and laptops are used in accordance with the Home Working policy.
- Do report any errors or problems promptly – If you have an error or an issue, especially if it may be security related, please report it to the IT Team quickly and with as much detail as possible. Reporting that you had a problem 3 days ago and you can't remember the error message makes it almost impossible to track and correct the problem. Reporting promptly with details of which system (e.g. terminal server, e-mail) was affected, the date and time the problem occurred and the specific error message or event makes it much easier to find and fix the problem, and get you working again.
- Do think about what you are saving and copying onto the network and in e-mail. Does the file need to be there? How big is it? If you are saving an attachment out of an e-mail, remember to delete the copy in the e-mail to save using up double the space. If you are copying data from an external storage device, why is this necessary? If it is only for your use, can it stay on the same?
- Do take care of the equipment you are issued with, either permanently or on loan. Most of it is expensive and it may contain sensitive or confidential data.
- Do remember to return the equipment before leaving MHC. All data will be securely erased by the MHCPL IT department. Please note that any personal data that has not been erased from returned equipment may be viewed by the IT department.
- Do keep passwords secure and never disclose them to anyone else. Passwords should ideally contain at least 9 characters with a mix of letters and symbols in upper and lower case.
- Do keep portable media, especially laptops, taken outside MHCPL offices secure at all times. For example, do not leave them in boots of cars overnight, in overhead luggage racks or unattended in other insecure areas. Where possible carry IT equipment in anonymous cases without a manufacturer's logo and avoid using laptops in public places where possible if confidential information may be visible to other people.

- Don’t connect any equipment (Laptops, USB devices including storage devices, networking equipment, data cards etc.) to MHCPL IT systems unless it has been supplied or specifically authorised by the MHCPL IT department. If in any doubt, confirm with the IT Team before connecting anything.
- Don’t download any Software, Software updates, Installation Packages, or Executable files from the Internet or external storage devices (USB sticks, external hard drives, CD-ROM, DVD etc.) onto MHCPL IT systems unless specifically authorised by the MHCPL IT Department.
- Don’t install any software on any MHCPL IT systems unless specifically authorised by the MHCPL IT department. All software installs are normally carried out by the MHCPL IT department and user installation of software is only authorised in special circumstances.
- Don’t download, upload, store, copy or distribute any materials, data or software of a obscene, indecent, racist, defamatory, libelous, offensive or otherwise unlawful nature (other than for properly authorised and lawful research, for which written notification must be given to the relevant HOD).
- Don’t attempt to circumvent the security and restrictions in place on the MHCPL IT systems. These are in place to ensure a safe working environment for all staff and maintain the security and resilience of the MHCPL network.
- Don’t leave portable media unattended in public places where there is a potential for opportunist theft or compromise (i.e. installation of a virus).
- Don’t connect any MHCPL issued equipment or storage devices into another computer or network unless you are happy the network is correctly maintained and up to date Anti-Virus protection is in place. Viruses can be transferred using machines and storage devices connected to compromised computers or networks.
- Don’t use the MHCPL network, including E drives, for the storage of music files, as these may breach copyright permissions. Private photographic and or video files should not be stored on E drives as they use up large amounts of space. For further information and advice please contact the MHCPL IT department.

3. Appendix B

Version Control Sheet

Version	Date	Author	Replaces	Comment
Initial	Mar15-2018	IT Manager	None	
Revision 01	Dec18-2019	IT Manager	None	
Revision 02	Jan02-2024	IT Manager	Cybercrime standards included