IT POLICY (Version 1.1)

Purpose

The purpose of this policy is to ensure business continuity and to minimise operational damage by reducing the opportunity for and impact of IT security incidents.

Scope

This Policy applies to all IT-related systems, hardware, services, facilities and processes owned or otherwise made available by The Health & Education Co-operative or on its behalf, Including the utilisation of cloud based servers and services and environments.
This policy includes any personally owned devices that are used in connection with our Business activities.
This policy applies to all employees and contractors who work for or on behalf of The Health & Education Co-operative Ltd.

Version Record

Version	Next Review Date	Reviewed By
V 1.0 Original Document	12/01/2022	Joanna Tate
V 1.1 Updated to include reference to anti-malware requirements for Mac	10/10/2023	Joanna Tate Tom Stack

Precautions against hardware, software or data loss

Your Computer must be safeguarded appropriately, especially when left unattended (e.g. locking your computer when leaving it unattended, even for a brief period of time).
Files downloaded from the internet carry a risk and should only be downloaded from trusted sites and should be scanned with an anti-virus product. Email poses a significant threat and files attached to and links within email must be treated with caution to safeguard against Phishing type attacks which seek to harvest personal information and deliver malicious code including ransomware that can lead to the encryption of important business data. You have a duty to check the address of the recipient each time an email is sent to reduce the chance of accidental data loss through email.

Individuals should not use automatic forwarding of email from their company email account to personal email accounts where there is the possibility for confidential or sensitive information being delivered to their work mailbox. Many personal email accounts will reside in Countries without UK equivalent data protection laws and are therefore inappropriate for certain classifications of our business data.

The use of USB storage devices is strongly discouraged as this is a common cause of compromise through infections from computer viruses, malware and spyware. We encourage you to use Google Drive for the storage of Documents and Files.

Storage devices which are not from a trusted source must not be attached to a company issued or personal device. Files on trusted USB storage devices must be scanned with an antivirus product before the files are accessed; Your Antivirus may prompt this action upon inserting the device into your computer.

Loss or Theft of your personal computing devices is another risk our business faces so we ask that you also utilise the features built into your Operating System. All Windows Users should enable the use of Bitlocker and Mac Users should use FileVault to encrypt their HardDrive(s).

Guidance on encrypting local storage on your devices can be found within these links:
Mac OS: https://support.apple.com/en-us/HT204837
Windows:https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d

Working Practices

Employees/Contractors must log out or lock their computer when not in use.
Screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons.
This applies to both fixed desktops and Laptops. Additionally, screens should be positioned so that they are not easily visible through external windows. Whilst sharing screens on video conferencing and collaboration platforms (Google Meets, Zoom etc) additional care should be taken to ensure sensitive information cannot be viewed on your screen or within your working environment by unauthorised persons.

Cloud Storage

Cloud storage introduces complexities relating to where data is stored and this is often in Countries without UK equivalent data protection laws. Sensitive or confidential information must not be kept in a cloud storage service which is not approved by The Health & Education Co-operative.
Due diligence must be undertaken to assess the risk to sensitive and confidential data before being uploaded to cloud-based storage and systems.
File Transfer services such as WeTransfer for any business or sensitive information and data. This is not an appropriate way to transfer such sensitive data.

Google Suite (Google Drive) is the approved storage platform for all your files related to your work.
Do not upload personal files and contents to this cloud storage service that are not for work purposes.

Backup and recovery

We ask that you store all files required to do your job in Google Drive, This avoids the need for creating and maintaining backups of your files on your personal computer for business purposes.
This information will be kept safe and backed up by Google and therefore it is best practice to keep all business files in Google Suite (Google Drive).

Backups of the business' information assets that run our services and the ability to recover them are important priorities. Our Senior Developer is responsible for ensuring that the backup and recovery procedures are in place for our websites/services and should ensure that these are stored safely.

Backup copies of data must be protected throughout their lifecycle from accidental or malicious alteration and destruction, particularly against the threat of ransomware for which offline backups are ideal to have in addition to online frequent backups. We keep an offline backup that is kept on an encrypted hard drive and stored away in a lock box for safekeeping and to avoid the data falling into the wrong hands.
Access to data backups and supporting infrastructure must be restricted to those persons who are authorised to perform systems administration or management functions.

Use of Electronic Communication Systems

Google Drive provides greater security through granular access rights management and the ability to revoke access to shared information at any time.

The identity of online recipients, such as email addresses should be checked carefully prior to sending, especially where the information content is sensitive or confidential. Verifying the correct document has been attached to an email prior to sending will reduce the opportunity for sensitive data loss via email. In most cases an email and its attachments cannot be revoked once sent externally.
Sensitive or confidential information should only be sent via email to external contacts where modern methods are not possible to external recipients and must be encrypted or protected by a password.

Information received electronically must be treated with care due to its inherent information security risks.
Files received from external persons should be scanned for possible viruses or other malicious code.

Irrespective of ownership, computers or other devices should only be used for business related activities if adequate protection is in place and policies are followed.
Personal computers used for business purposes should be deemed acceptable for use by Joanna Tate in accordance with our policies and guidance. Staff and Contractors should take steps to ensure other users of the equipment cannot view or access business information. They are responsible for ensuring all devices adhere to the highest levels of security.

Any loss or theft of computing equipment (business issued or personal equipment) which has been used to access sensitive Business data must be reported to Joanna Tate at the earliest opportunity.

Securing your accounts

We require that you use strong passwords for all of your accounts, especially your computer account, computer Administrator account and any other accounts used in relation to your work with The Health & Education Cooperative. Password quality is important to ensure your accounts are secure against attacks by cyber criminals such as brute force attacks or those who may try to guess your password. Please ensure all your passwords are secure and use at least 8 characters with a combination of Capital Letters, Lowercase and Special Characters.

It is recommended that you change your computer password frequently to ensure it is secure.
If you are contacted about a breach of a service you use we ask that you follow the reporting concerns procedure immediately and action a password change for the relevant account(s) as quickly as possible.

2 Factor Authentication (2FA / MFA) is highly recommended for use on all of your accounts where it is available. MFA is a helpful tool to verify that you are the account holder and also to act as a second defence against weak, shared or compromised passwords.
2 Factor Authentication is enforced for access to Google Suite (Google Drive). It is also a mandatory requirement for any Administrative accounts, especially for Administrators of AWS. We ask that you ensure you activate it on all of your accounts that allow it.

The Senior Developer should ensure that passwords are changed when compromise is suspected.
The monthly Security Audit is designed to ensure that we are on-top of such matters as frequent password changing and patching of systems.

Personal Equipment (Computers, Smart Phones and Routers)

Mobile Devices
Mobile Devices (smartphones and Tablets) are forbidden for accessing company email and files. Laptops and Desktop computers should only be used for work purposes. Any mobile Devices detected accessing their company account will be immediately blocked by Joanna Tate from any future access on that mobile device (via Google Admin Console).

Personal Computers
We recommend that you change the BIOS password of your personal computer to prevent any unauthorised changes to your BIOS settings.

Auto-Run must be disabled on your computer. This is to prevent anything from inserted media (CD, USB Drive) or downloaded executable files from running by themselves before you have had the opportunity to scan them with an Anti-Virus first. Disable Auto-Run for Windows:
https://support.microsoft.com/en-us/topic/how-to-disable-the-autorun-functionality-in-windows-8e5ff0da-c526-7624-c064-ff82aecfd145#:~:text=Under%20Computer%20Configuration%2C%20expand%20Administrative,Restart%20the%20computer.

Windows Computers should have an Anti-virus software installed to offer additional security against threats. Windows Defender is adequate for Anti-Malware but you are welcome to request a licence for our chosen Anti-Malware solution if you wish.

For Mac Computers we require you to use an Anti-Malware solution to offer adequate protection. Malwarebytes is our current preference for this solution for Anti-Malware.

We strongly recommend that you do not allow others to share or access your computer.
If others do use your computer then please ensure that they only have access to a ‘standard’ level of account.
It is strongly recommended that you only have ‘necessary’ accounts and avoid ‘guest accounts’ that may allow open access to your computer.

Software
It is important that you remove any unnecessary and unused software on your computer.
We ask that you run frequent security scans on your computer to detect any PUA’S (Potentially Unwanted Applications).

Operating System
It is important to check that your computer is running the latest version of the Operating System you use for your computer to ensure that it is as secure as possible and working to its full potential. You should ensure that these updates are set to run automatically or updates are manually checked for daily if not possible to auto-update.
We remind everyone during our Security Bulletin emails (attached to our Team Meeting Minutes) to ensure that you have run these updates; We understand that it can be tempting to avoid updating due to the additional time this takes but it is highly important that you allow these automatic updates to run.
Your Anti-Malware solution (Malwarebytes) runs in real time but we ask that you schedule scans for the start of your working day (9am typically) and schedule it to check for updates every 3 hours at minimum.

Personal Networking Equipment
It is your responsibility to ensure that the default admin password of your router/hub (ISP Issued device) has been changed from the default password. We recommend that you change this at least once a year.
It is important that you change this password immediately if your ISP Provider/the manufacturer issues a statement informing you that there is a compromise.

It is also recommended that you check which devices are connected to your WI-FI frequently to ensure that others who should not have access to your home internet are not accessing it. It is not a requirement to change your home WI-FI Password but we do recommend that you change the default WI-FI password too for additional protection.

Reporting Concerns

If you are concerned that there is a security incident or suspected weakness on your personal device or within the Organisation you should immediately notify Joanna Tate. It is important that these concerns are reported in a timely manner so that we can react appropriately to minimise potential damage or disruption. These concerns include but are not limited to any vulnerabilities you are aware of within programming languages and Operating Systems (Computers and Servers), your personal home equipment (home router etc).

The Senior Developer will act on any reports of concern raised by Joanna Tate . The Senior Developer will make the appropriate changes to minimise risk. Reported concerns and any actions taken are recorded and logged on a spreadsheet maintained by Joanna Tate. If appropriate the information will be shared during our Team Meetings but not until the issue has been resolved.

Change Management

Changes to operational procedures, software or hardware must be controlled to ensure continuing compliance and must have management approval from Joanna Tate.

User Management

System Owners are encouraged to create a separate user account on their computer that is of a 'standard' permission level. This is to separate their personal account with personal contents from their work they do for us and also prevents any attempts of exploiting admin privileges within the computer without first raising a request for Admin privilege to run. We ask that this account is secured with a strong password and that they are the sole user of that account and computer if/where possible and that any other individuals accessing the computer do not have a higher level of permission than the individual who owns it to prevent access to this account for work purposes.

Administrators of Servers (AWS) should not install or attempt to host additional unnecessary files for non business related purposes. Admin's may not install any software on the server that does not relate to serving http content. Installing an OS GUI, a web browser or email client is strictly prohibited

Misuse of systems is not acceptable - Your account and any AWS Access should only be used for HEC related business activities as approved by Joanna Tate.
It is important that you logout of your Administrator account as soon as you have completed your tasks.
Account access to any Servers must first be authorised by Joanna Tate using the ‘System Access Request’ form which is also used for account tracking in line with HR procedures and records.

Starters & Leavers

Access to systems / service management should only be available to current employees during their period of employment. In particular, line managers must ensure that access to all systems is withdrawn as soon as a staff member's employment is terminated or amended should their role change. Requests for changes are made by completing and filing a 'System Access Request' form.

Those requesting change due to a role change within the business must ensure that system access does not extend beyond the requirements of the individual and their new role. The process of Account Tracking is processed via Human Resource and the Senior Developer who are both responsible for recording and maintaining the log of access for Employee accounts.

Upon an individual leaving their employment with The Health & Education Cooperative should return any equipment that we own. Line Managers are responsible for ensuring their access is terminated on their final day of employment.

This policy is next subject to review on/before: 10/10/2023