The NHS Confederation

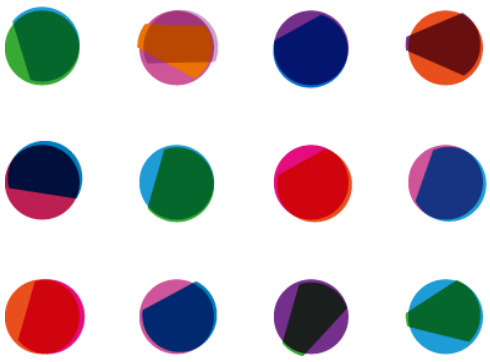
Charity number 1090329

Company number 04358614

IT Security Policy and Procedures

Date policy agreed by Board of Trustees	October 2020
Date of policy review:	October 2022
Owner of policy:	Director of Finance and IT

CONTENTS



The voice of NHS leadership

1. INTRODUCTION

The organisation provides access to a range of electronic facilities and equipment which are intended to assist employees in the performance of their duties. These facilities are an integral part of how we work.

This policy sets out the NHS Confederation's position and arrangements for the installation and use of IT facilities and equipment including dealing with any abuse. Responsibility for the implementation and monitoring of this policy is the responsibility of the IT and Facilities Manager.

This policy is intended to protect the organisation's information, assets and reputation as well as the rights of every employee. It applies equally to every employee and all other persons logging on to the organisation's equipment or accessing the organisation's domain and network. If third parties, such as secondees or consultants, are given access to the network, it is the responsibility of the staff member who appoints them to inform them about this policy.

2. PURPOSE

The principal reasons why this policy must be followed in all circumstances are:

- The NHS Confederation is legally responsible for all software on the organisational devices. The IT team maintain records of the licences purchased and ensures the organisation operates within the limits permitted by the number of licences owned.
- The software being used within the organisation can be audited at any time by the supplier, without notice. The NHS Confederation would be prosecuted if found to be using software without the correct licensing arrangements.
- There is the risk of a virus being picked up from any software installation or from the connection of any piece of hardware. Because the organisation is networked, a virus that contaminates one machine can quickly spread across sites and fileservers. This poses the risk of causing significant damage and loss of information across the organisation.
- There is the possibility that the installation and use of any piece of software will adversely affect the performance of the machine(s) on which it is installed. Programs may not run properly or may conflict with each other. Machines may crash or run poorly. The IT team therefore needs to evaluate any proposal to use new software before making it available
- If a member of the IT team identifies any unauthorised software on any equipment owned and operated by the NHS Confederation, it will be removed immediately.

- This policy should be read in conjunction with:
    - Acceptable use
    - Procurement of IT
    - Bring your own device (BYOD)
    -

3. CONTROL MEASURES AND POLICY STATEMENTS

3.1. Passwords and PINs

- Passwords are required for each user to be able to access the network (email, OneDrive, shared drives). Users are required to change their password every 90 days. Passwords are required to be at least 12 characters long. Passwords must be a mixture of upper and lower-case letters, numeric and symbols. Password history has been set at 8 so a password cannot be re-used until 8 others have been set and used. Users are given 14 days' notice to change their passwords.

- To ensure the highest levels of security possible, all staff are reminded that all passwords for the network and software are not to be shared with anyone else, either inside or outside of the organisation. Sharing your password will be dealt with under the disciplinary policy and procedures.

- If colleagues need to access email whilst users are away, line managers should contact the IT helpdesk and delegated rights can be issued.

- If you believe that your password has been compromised or someone else has been using your login details, change your password immediately and inform your line manager as well as the IT helpdesk.

- Only the IT team have admin passwords needed to make changes to devices and infrastructure.

- All mobile devices are required to have a PIN in place. PINs are automatically set up for Samsung android devices. For devices under the BYOD policy, PINs must be a minimum of 4 digits.

3.2. Firewalls and Virtual Private Network (VPN)

- The NHS Confederation will always maintain firewalls to enhance IT security. The firewalls are installed and configured to protect the network from outside attacks.

- The NHS Confederation will ensure that a VPN (Global Protect) program installed onto all laptops and PCs. This is to create a virtual encrypted connection from the user's local machine to the network. Connection to the network ensures that security policies are pushed out to the local machine. With an authenticated connection, users are connected to the shared drives (if they are still in use), printers and the Microsoft Azure cloud environment.

- In addition to the firewalls mentioned above, all devices are protected by locally installed BitDefender firewall, which is set up as part of the build process.

3.3. Anti-Virus protection

- The organisation uses an anti-virus solution from Bitdefender. This provides desktop and server-level protection against viruses. The software is automatically updated with virus definitions as they are made available.

- A virus is a piece of self-replicating code, most often a malicious software programme designed to destroy or corrupt information, steal user data or adversely impact the usage of IT systems.

- Potential sources of viruses include shared media such as USB memory sticks, email (including, but not limited to, files attached to messages), malicious code embedded in websites and software or documents copied over networks such as the internal network or the internet.

- An infection by malicious software can be very costly to the NHS Confederation whether through the loss of data, staff time to recover a system or the delay of important work. In addition, viruses spread from the NHS Confederation could potentially lead to damage to our reputation and possible legal action.

- All computers connected to the NHS Confederation network must run an approved, licensed and up-to-date anti-virus product that continually monitors for malicious software.

- All active directory domain-based computers must run the centrally managed virus protection software.

- Privately owned computers that connect to the NHS Confederation network must be equipped with an appropriate anti-virus product and be checked by the IT

team in line with the Bring Your Own Device (BYOD) Policy. The NHS Confederation does not allow personal or non NHSC laptops or devices to connect to the Azure environment.

- The NHS Confederation reserves the right to disconnect any machine from the network if an infection is found or suspected. The machine will remain disconnected until the infection is removed.

3.4. Internet and email security

- The organisation uses Mimecast as its internet and email security solution. This allows the IT team to monitor and report on usage, along with protecting the organisation against malicious websites and emails.

- The Acceptable Use Policy gives more information on conditions of use for internet and emails.

3.5. Access control

- The IT team manage all NHS Confederation devices using Mobile Device Management (MDM) which enables the team to report on what software is on laptops and the versions of these. The organisation uses Intune and Mobile Iron MDM systems which notify IT if any updates or software patches have not taken place on devices.

- IT staff may have access to management and security systems which gain them access to information not commonly available to all staff. Any information accessed in this way must be kept completely confidential. Examples of this include access to the email filtering systems, staff mailboxes and personal details.

- Administrator accounts should only be used for specific administration purposes. These accounts should not be used to carry out the staff member's day to day work such as writing documents or checking emails. Administrator details must not be shared with anyone outside the IT team.

- Any high impact, and or, high risk changes, must have a change control document completed and approved by the IT manager.

3.6. Backups

- The organisation is required to deal with its data in a way that meets legal standards. The organisation keeps a back up of all corporate data.

- Backups of data from the shared network drives (Z and P) are taken automatically by Azure each night and stored within the organisation's cloud infrastructure. Multiple, historical versions of all files from the main network drives are kept.
- Backups of data from Exchange, OneDrive and Sharepoint are taken automatically by Barracuda Cloud Backup each night and stored within Barracuda's cloud infrastructure for 7 years.

- Version History is enabled on Sharepoint document libraries. The previous 50 versions of documents are saved in a 'version history' across our SharePoint sites.

- Deleted items from SharePoint Libraries and OneDrive for Business are stored in the recycle bin for 93 days. After this they are recoverable through Barracuda.

- Deleted emails are stored in the individual's deleted items folder of their inbox for 30 days. After this they are recoverable through Barracuda.

- Backup logs for virtual machines, network drives (Z and P) and Barracuda are checked each day to ensure that the backups have been successful. At least once a month a test is carried out to ensure that data from shared drives can be restored successfully.

- Documents saved on a desktop are not backed up and the IT team cannot guarantee recovery if files are lost. It is recommended that documents are instead saved to OneDrive as these are backed up by Barracuda as noted above.

- Refer to the Data Retention Policy for more information.

- The IT team ensures that business continuity plans and impact assessment, and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

3.7. Autoplay and external hard drives

- Autoplay has been disabled on all devices to protect against malware.

- External hard drives and USB sticks must be tested by IT prior to use. Once tested and confirmed as virus free, the device will be encrypted and added to the approved device list.

4. RESPONSIBILITIES

4.1. IT Team responsibilities

- Developing, implementing and enforcing suitable and relevant information security policies and procedures to ensure NHS Confederation's systems and infrastructure remain compliant with the Data Protection Act 2018 and GDPR.
- At achieve and maintain the Cyber Essentials Plus accreditation.
- Maintain the IT infrastructure - monitoring network health, patching and updating, and responding to security alerts.
- The IT team manage all installation of hardware to ensure that it is set up correctly.
- Only the IT team can install software onto equipment owned by the NHS Confederation. This applies to office-based and home-based equipment and mobile devices.
- IT or telecoms equipment used by staff can only be installed, connected and configured by the IT team.
- The IT team will investigate any incidents of security breaches and will report any situations where sensitive or secure data has been misused or transferred without authorisation. These events will be escalated to HR to be handled through the disciplinary procedure, if appropriate.
- Work with the staff to manage their access permissions e.g. if temporary access to a mailbox is granted, it should be removed when access is no longer needed.
- Maintain the approved encrypted media list.

4.2. All staff responsibilities

All staff are responsible for:

- Being aware of the contents of each of the IT policies

- Taking suitable measures to protect against virus infection and phishing attempts including:
    - Not opening suspicious emails and deleting suspicious emails
    - Not opening email attachments from unknown or unreliable sources
    - Not interacting with “clickbait”
    - Accessing only work-related websites and not accessing inappropriate sites.
    - Not using unencrypted USB sticks (or only using encrypted USB sticks authorised by IT)

- Reporting suspicious emails and or activity in the network in the following way:
    - Forward suspicious emails to ithelpdesk@nhsconfed.org. The IT team will investigate as a priority and respond to concerns raised.

- Reporting lost or stolen IT equipment in the following way:
    - Staff must notify IT and their line manager as soon as possible if a device is lost or stolen.
    - The external number for the IT team is 0844 800 5985.

- Reporting a potential breach of this policy in the following way:
    - Email the details to ITsecuritybreach@nhsconfed.org. IT Manager, Assistant Director of Finance and IT and Governance Manager have access to this mailbox and will investigate.

- Work with the IT Team to manage their access permissions e.g. if temporary access to a mailbox is granted, it should be removed when access is no longer needed.

4.3. Manager responsibilities

- Managers are responsible for approving access requests for their staff and for being aware how long the access is required for. Access approval must be in writing to the IT Helpdesk accompanied by an appropriate justification, based on the requester’s business need.

- Managers are expected to review team members permission levels on a regular basis. The manager is able to contact IT for this information.

- Complete ‘Starter Form’ and ‘Leaver Form’ informing the IT team of requirements for staff joining and leaving the organisation.

- Discuss breaches to this policy with the IT Manager and Assistant Director Finance, Contracts and IT.

5. MANDATORY STAFF TRAINING

Information Security awareness training is mandatory for all staff to complete via the online training portal. The training covers some of the areas covered in this policy such as:

- Strong passwords
- Locking your computer if you leave your desk
- Securing personal devices (BYOD Policy)
- Working outside the office
- Reporting procedures