The NHS Confederation

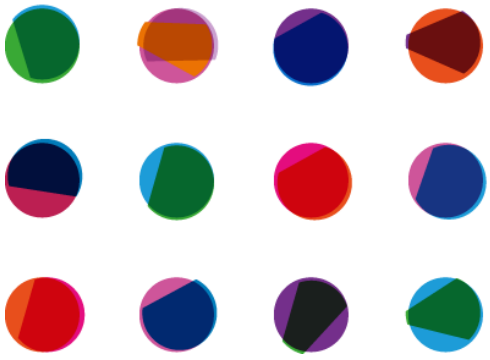
Charity number 1090329

Company number 04358614

Acceptable Use Policy

Date policy agreed by Group Executive:	October 2020
Date of policy review :	October 2022
Owner of policy:	Director of Finance and IT

CONTENTS



Introduction

Purpose of this policy

The NHS Confederation provides access to a range of electronic communication facilities to promote and enable a positive and extensive use of IT to support the delivery of our business and the fulfilment of our charitable objectives. These facilities are an integral part of our daily communications and the key mechanism by which we exchange information with each other and with external contacts. This policy details the conditions of use and the expected behaviours of those with access to the NHS Confederation's systems.

Scope

This policy applies to everyone working at or with the NHS Confederation[1] that use the NHS Confederation's systems and equipment. It applies to:

- all staff, including chief executives, directors, senior managers, employees (whether permanent, fixed-term or temporary), seconded staff, homeworkers, agency workers and volunteers;
- consultants and contractors;
- board and committee members.

Any employing or contracting manager must ensure that all temporary staff, consultants, or contractors are aware of this policy.

By the NHS Confederation we mean the NHS Confederation charity, any subsidiary companies and any networks or country arrangements.

The NHS Confederation has designated the Director of Finance and IT as the individual who is responsible for ensuring that the NHS Confederation implements this policy.

This policy should be read in conjunction with the organisation's IT policies:

- IT Security Policy
- Bring Your Own Device (BYOD) policy
- Procurement of IT policy
- Data Breach Policy and Procedure
- Social Media Policy

[1] Collectively referred to as workers in this policy

Policy statements

Computer Access Control

Access to the NHS Confederation IT systems is controlled by the use of usernames and passwords. All user authentications are uniquely assigned to you as an individual and consequently individuals are accountable for their actions on the NHS Confederation's IT systems.

Individuals must not:

- Allow anyone else to use their NHS Confederation IT equipment.
- Allow anyone else to use their user ID and password on any NHS Confederation's IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access NHS Confederation IT systems.
- Leave their password unprotected, for example writing it down.
- Perform any unauthorised changes to NHS Confederation IT systems. If in doubt, individuals should contact the IT team.
- Attempt to or access data or documents that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data or documents.
- Connect any personal device to the NHS Confederation's network or IT systems, unless authorised as part of the BYOD policy. Please note, mobile phones should be connected to the guest WIFI when in the office, not the corporate WIFI (NHSC WIFI).
- Connect any external memory device to NHS Confederation IT equipment, unless this has been authorised by the IT team and the device is encrypted.
- Store any NHS Confederation data on any non-authorised NHS Confederation equipment.
- Give or transfer the NHS Confederation's data or software to any person or organisation outside NHS Confederation without the authority of NHS Confederation.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data. Failing to comply with these policies may result in disciplinary action.

Internet and Email Conditions of Use

Use of the NHS Confederation internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the NHS Confederation in any way, not in breach of any term and condition of employment and does not place the individual or the NHS Confederation in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in any electronic communications.
- Access, download, send or receive any data (including images), which the NHS Confederation may consider offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list).
- Use the internet or email for personal gain or to conduct personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the NHS Confederation, alter any information about it, or express any opinion about the NHS Confederation, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally without the authority of NHS Confederation.
- Forward any NHS Confederation data to personal non NHS Confederation's email accounts (for example a personal Hotmail or Gmail account).
- Make official commitments through the internet or email on behalf of NHS Confederation unless authorised to do so.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download or install any software from the internet without prior approval of the IT Department.
- Send excessive personal emails or sign up to non-work related online services using their NHS Confederation email address.

Working off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment taken off-site must not be left unattended in public places.
- Equipment must not be left in sight in a car during the day and must not be left in a car overnight.
- Information is protected against loss or compromise when working remotely. Backups with version history can be provided by IT if needed and staff should utilise OneDrive and Sharepoint.
- Particular care is taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They are protected by a password or PIN in line with the IT Security Policy.

Software

Employees must use only software that is authorised by the NHS Confederation on NHS Confederation devices. Authorised software must be used in accordance with the

software supplier's licensing agreements. All software on NHS Confederation computers must be approved and installed by the NHS Confederation's IT Team.

Individuals must not:

- Store personal files such as music, video, photographs or games on NHS Confederation IT equipment.

Anti-Virus Software

The IT team has implemented centralised, automated virus detection and anti-virus software within the NHS Confederation. All laptops have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved NHS Confederation anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of NHS Confederation's voice equipment (including the telephony systems and Teams facilities) is intended for business use. Individuals must not use NHS Confederation's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances.

Individuals must not:

- Use NHS Confederation's voice facilities for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

Monitoring and Filtering

All data that is created and stored on NHS Confederation computers is the property of the NHS Confederation.

IT system logging of activities will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The NHS Confederation has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Actions upon leaving the organisation

All NHS Confederation equipment and data, for example laptops and mobile devices including telephones, smartphones must be returned to the NHS Confederation no later than your last day of employment.

Responsibilities

IT team

- To maintain security systems, monitor use, investigate instances of misuse and escalating as appropriate.
- To review this policy annually to ensure compliance with Cyber Essentials accreditation.

Individuals

- To abide by the policy terms and to report suspected breaches of this policy or the IT Security Policy without delay to your line management and the IT team.

Group Executive

- To deal with escalated issues and breaches of this policy.