NHS Confederation

Acceptable use Policy

Charity number 1090329

Company number 04358614

Owner of policy	Director of Finance & IT
Date of policy review	April 2024
Approved by CEO	April 2024
Agreed with Joint Negotiating Committee	May 2024 meeting
Next review date	April 2025

Contents

Version Control:

Version	Date	Changes
1.0	October 2022	Updated policy
1.1	April 2024	Review and amendments

1. Scope

This policy details the conditions of use and the expected behaviours of those with access to the NHS Confederation's IT systems and the appropriate use of those systems. This policy should be read in conjunction with all other IT policies.

This policy applies to all staff and users who access NHS Confederation's IT systems and equipment including chief executives, directors, senior managers, employees (whether permanent, fixed-term or temporary), seconded staff, agency workers, consultants and volunteers. For the purpose of this policy all roles covered in the scope are referred to as 'users'.

2. Computer Access Control

Access to the NHS Confederation IT systems is controlled using usernames and passwords and multi factor authentication (MFA). All user authentications are uniquely assigned as an individual and consequently individuals are accountable for their actions on the NHS Confederation's IT systems.

All users are managed through the joiners, movers, leavers process and access is not granted without the correct paperwork. Access can be changed or revoked as required by the organisation. Upon leaving the organisation, access will removed within 5 days of notifying Stripe.

3. IT system 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 and 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 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 or encryption of NHS Confederation.

- Forward any NHS Confederation data to personal non NHS Confederation 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 team.

- Send excessive personal emails or sign up to non-work related online services using their NHS Confederation email address.

4. Remote working

Equipment must not be left unattended or unsecured 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 must be protected against loss or compromise when working remotely.

5. Use of personal mobile devices

Personal devices can be used for work purposes – see Bring Your Own Device (BYOD) policy. When using personal devices, application data is owned and controlled by NHS Confederation. NHS Confederation has the right to wipe the data within any M365 application on a personal device.

6. Software and data

Users must use only software that is authorised by the NHS Confederation in the approved list of the Software Policy on NHS Confederation devices. Authorised software must be used in accordance with the software supplier's licensing agreements. Individuals must not download non-business data such as music, video, photographs or games on NHS Confederation IT equipment.

7. Anti-Virus Software

All laptops have antivirus software installed to detect and remove any virus automatically. Users should not disable or attempt to remove any anti-virus software.

In some instances, antivirus software may not automatically address an issue. Users should contact Stripe OLT (service@stripeolt.com) immediately if they see unusual behaviour or messages on their screen.

8. 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.

9. Monitoring and Filtering

IT system audit logging is in place for all systems. 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 all activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

10. Actions upon leaving the organisation

It is the responsibility of line managers to ensure that all NHS Confederation equipment is returned by their employee no later than the last day of employment.

11. Failure to comply

All staff must ensure that they read, understand and comply with this policy. Failure to comply with this policy may result in disciplinary action.

12. Responsibilities

12.1 Director of Finance and IT

- To deal with escalated issues and breaches of this policy.
- Investigate instances of misuse and escalating as appropriate.

12.2 Stripe OLT

- Manage requests for access to NHS Confederation systems.
- Assigning role-based access controls.

12.3 Line Managers

- Must ensure that their teams are given clear training on relevant IT systems and how best to use them in accordance with their role.

12.4 All staff

- To ensure no one aside from themselves has access to use their NHS Confederation IT equipment.
- Ensure log in and password are kept secure for all accessible systems and not shared with any other person.
- To ensure devices are left locked when unattended at any time, in any location.
- To not allow anyone else to use their user ID and password on any NHS Confederation IT system.
- Not use someone else's user ID and password to access NHS Confederation IT systems.
- Not attempt to or access data or documents that they are not authorised to use or access.
- Not exceed the limits of their authorisation or specific business need to interrogate the system or data or documents.
- Not connect any personal device to the NHS Confederation's network or IT systems, unless authorised as part of the BYOD policy.
- Not connect any external memory device to NHS Confederation IT equipment.
- Not store any NHS Confederation data on any non-authorised NHS Confederation equipment.
- Not give or transfer the NHS Confederation's data or software to any person or organisation outside NHS Confederation.
- To abide by the policy terms and to report suspected breaches of this policy or any other IT Policy without delay to your line management and the IT team.

Equality Impact Assessment - Policies

The following guidance and checklist provides a framework for Equality Impact Assessments (EIA). It should be used when carrying out equality impact assessments (EIA) in relation to any new or revised policy. The checklist will help in considering the impact of the policy in relation to equality and diversity (E&D).

The Checklist is to be used for any new or revised policy, not just those that appear to have high relevance in relation to equality and diversity issues. Completion of the Checklist does not need to be a time-consuming or difficult process but should raise some important questions as you carry out the process.

Name of policy being assessed	Bring Your Own Device (BYOD) Policy
Policy Owner	Director of Finance and IT
EIA completed by	Director of Finance and IT
Date Completed	April 2024
Summary of purpose of the policy	To provide guidance around the use of personal devices to carry out NHS Confederation work
Who are the main stakeholders and what involvement and consultation have they had in the policy development. Include staff groups, trade unions and board committees as applicable.	All staff
Who is affected by the policy	All staff
What are the arrangements for monitoring and reviewing the actual impact of the policy	Continuous monitoring by the SOC team to ensure adherence to this policy.

Please indicate against each of the following protected characteristics, what the impact of the policy would be and actions that will be / have been taken to mitigate any negative or adverse impact identified.

(Where the policy is found to have either a positive or negative impact on a particular group it will need to be reviewed or justified within the permits of the law.)

Protected Characteristics	Impact Y/N	Action(s) you will take to mitigate or remove the negative or adverse impact if identified?	Action Owner
Age *Consider impact on young people, older people etc.*	N		
Disability *Consider people with physical disabilities, hidden disabilities and neurodiversity.*	N		
Gender Reassignment *Consider people undergoing or have undergone gender reassignment*	N		
Pregnancy and Maternity *Consider those who are pregnant and those on pregnancy and parenthood leave. Consider those wishing to take parenthood leave*	N		
Race / Ethnicity *Consider potential impact on people from different ethnic groups and nationalities.*	N		
Religion or Belief *Consider people with different religious, faith and non-beliefs*	N		
Gender *Consider all genders.*	N		
Sexual Orientation *Consider LGBTQ+ people.*	N		
Marriage and Civil Partnership	N		

Consider marriage and civil partnership in respect of the due regard to the need to eliminate unlawful discrimination in employment.			
Does the policy promote fairness and equal opportunities? Provide details.	Yes, the policy is applicable to all workers equally and fairly		

Manager Signature: NBarraclough	HR Review Signature:
Date: 4/6/24	Date: