


UHL Apprenticeship and Development Centre IT Acceptable Use Policy

Centre Lead	Judith George Centre Education Manager - UHL Apprenticeship and Development Centre	
Written By	Judith George Centre Education Manager - UHL Apprenticeship and Development Centre	
Checked and Approved by Board Director Lead	Clare Teeney Chief People Officer	<i>Signature:</i> 
Consultation	UHL Apprenticeship and Development Centre	
Version	V1	
Supersedes	-	
Date of Original Approval	February 2019	
Next review Planned	March 2026	
Supporting Document(s)	<ul style="list-style-type: none"> • Safeguarding Policy • Inappropriate Behaviour Policy 	

Contents

1. Rationale.....	3
2. Purpose.....	3
3. Definitions	3
4. Internet use.....	3
5. User Responsibilities	4
6. Network Security.....	6
7. Raising a Concern.....	6
8. Unacceptable behaviour.....	6
9. Personal Equipment.....	7

Document Amendment and Review Log

March 2023	V1.5 Change of name and document format	16/03/2023	JS
April 2024	V1.6 Document branding updated	23/04/2024	JS

1. Rationale

The University Hospitals of Leicester Apprenticeship and Development Centre (here after referred to as the Centre) have access to ICT resources to support learning and development. University Hospitals of Leicester (UHL) who employs the Centre and governs its activities also owns the ICT resources and the master policies that govern their use. UHL has a duty of care to learners employed by both UHL and other health care organisations to ensure they use the internet and equipment correctly.

All access of computers and connected systems is governed by the Computer Misuse Act 1990. Any computer or digital technology used within the Centre for the education elements of the Apprenticeship Education Programme must be used in accordance with all other Trust policies; particularly the Email, IT Use, Trusts Anti-Bullying and Safeguarding Policies.

This policy covers the use of technology by learners/apprentices and visitors of the Centre.

The Centre will not tolerate the misuse of IT.

2. Purpose

- 2.1 The purpose of this policy is to provide guidance on what is deemed as acceptable and unacceptable use of IT by learners / apprentices whilst on education elements of their apprenticeship with the Centre.
- 2.2 The employment elements of a learner's / apprentice's apprenticeship and the use of IT within that will be governed by their employer's policies.
- 2.3 The Centre encourages the appropriate use of technology within the learning environment.

3. Definitions

- 3.1 Computer User:
A learner or visitor to the Centre using a computer, tablet, mobile phone, digital camera, MP3 player, mobile network "dongle" or any other digital technology.
- 3.2 Computer Facilities:
IT devices and networks that are provided to learners to access support, education and administration of the Centre.

4. Internet use

- 4.1 The Centre actively encourages the use of the internet by learners whilst on programme and, should they be required, provides laptops during study and project workshop days.
- 4.2 The Centre does not routinely monitor or inspect internet usage using Centre Equipment unless a good reason is provided. Inspections are carried out through Trust policies and with the support of the Subject Matter Expert.
- 4.3 The Centre reserves the right to inspect and/or monitor internet use when it has a reason to believe that a user has breached user privileges.
- 4.4 Anyone breaching the IT Use Guidelines may lose access rights and will be subject to investigation under the Centre's Misconduct and Disciplinary Procedures.

5. User Responsibilities

- 5.1 All users are expected to act responsibly and to show consideration to others. By using the Centre's computers or other devices, learners are agreeing to keep to the Centres Acceptable Use Policy.
- 5.2 The Centre's computers and network are not a place to store personal files such as movies, photographs or music files. Any such personal files could be removed without warning to conserve storage space for the proper use of the computers and network. Learners should not store assignments on shared computers.
- 5.3 Users must not do anything that will affect how the Trusts network performs or operates. For example, learners and visitors must not try to:
 - Download, store or install software onto computers
 - Introduce a virus or malicious code to the network
 - Bypass network security or other security systems, including the Trust's firewall
 - Access another user's account
 - Access an area or system they are not allowed to use
 - Use any form of hacking/cracking software or system
 - Connect a personal device to the network that acts as a Wireless Access Point (WAP) or router or a server
 - Connect any device to the network that has access to the Internet via a connection not provided by the Trust
 - Access, download, create, store or transmit material that is in conflict with the values or behaviours of the Trust or NHS, or their policies
 - Waste technical support time and resources
 - Send or forward chain emails
 - Send or forward emails to a large number of recipients
 - Open attachments from senders who are not recognized, or attachments which look suspicious.

- 5.4 Learners and visitors should ensure when using IT resources that they do not:
- Copy and use material from the internet to gain unfair advantage in their programme. Such actions may lead to disqualification by examination awarding bodies.
 - Break copyright restrictions when copying and using material from the internet. Copyright guidelines can be found in the copying room of the Centre within the Knighton Street Offices.
- 5.5 Learners and visitors to the Centre must ensure they:
- Protect the network
 - Keep their password secret and secure
 - Create a password that is not easy to guess by anyone else
 - Regularly change their password.
- NB: If any user suspects that someone else knows their password they will change it immediately and if a user accidentally finds out someone else's password they should advise the individual to change it or if not possible advise a member of Centre staff
- Use public messaging services such as Skype or Facebook only in support of learning activities
 - Communicate with people whom they know personally only
 - Do not make arrangements to meet people they have met on the internet
 - Never accept files or downloads from people they do not know, or which look suspicious
 - Do not attempt to repair equipment themselves
 - Do not create profiles or use a screen-name which is offensive, or gives away additional personal information
 - Do not add unnecessary or misleading personal information to their profile or account details
 - Respect the privacy of other users
 - Do not forward private data without permission
 - Respect all IT and associated policies of the Trust when using their own devices in paid time or unpaid breaks on programmes. These can be found on the Trust intranet site (Insite)
 - Only access systems and records they are authorised to do so
 - Delete spam messages
 - Raise any privacy concerns
- 5.6 Learners will use email systems responsibly and securely in line with organisational policies. Learners should note that:
- 5.6.1 The Centre actively encourages the use of email by both staff and learners.
 - 5.6.2 The Centre does not routinely monitor or inspect Trust email systems without good reason.
 - 5.6.3 The Centre reserves the right to inspect, monitor, or disclose emails through Trust procedures when it has a reason to believe that a user has breached the email privileges.
 - 5.6.4 Anyone breaching the email guidelines may lose access rights and will be subject to the Centre's and Trust's Disciplinary investigation procedure.
 - 5.6.5 An e-mail is not as secure or as private as may be perceived. Email, due to its very nature, is easily distributed due to the forwarding facilities within the e-mail software. A message

sent to one person can quite easily be forwarded to an unlimited number of people or could even be posted onto an electronic bulletin board or 'List Server.' Even when a user deletes their copy of the email, it may still exist in a backup file on the recipient's system or elsewhere on the internet. The Centre has no means of protecting against such eventualities.

- 5.6.6 Email created or stored on UHL Trust systems may be subject to disclosure during legal proceedings.
- 5.6.7 The Centre or Trust will not routinely disclose email without good reason. Users are cautioned against using emails to make any statements which they may not wish to be disclosed in the case of a dispute at a later date.
- 5.6.8 The Centre expects users to use the same personal and professional courtesies and considerations in e-mail as they would in any form of communication.
- 5.6.9 The Centre cannot 'authenticate' the origin of all email unless it is sent using an authorised email service.
- 5.6.10 The Centre requires users not to make any attempt to disguise the origin of their email. Any email that has been forwarded can be modified to hide its source; this again is against Centre policy.

6. Network Security

- 6.1 Learners and external verifiers will be set up with relevant IT access which could include access to Trust internet/intranet and/or ePortfolio systems (provided through Leicester College) as relevant to their needs.
- 6.2 UHL IT systems are filtered to prevent access to inappropriate content using several various methods.
- 6.3 UHL IT systems record of all the webpages visited by all users. Full details can be found on the UHL policy.
- 6.4 All users must understand that the Trust can and will access personal areas on the network in order to ensure the safety and security of all users. Privacy will be respected unless there is reason to believe that this Acceptable Use Policy or guidelines are not being followed.
- 6.5 Trust emails are automatically scanned to remove spam and inappropriate content.

7. Raising a Concern

During the education element of their Apprenticeship Education Programme, if any user receives an email which is in conflict with the values and behaviours of the NHS, or is offensive or upsetting, they should raise this with a member of Centre staff. The email in question should not be deleted until the matter has been investigated.

8. Unacceptable behaviour

In addition to the user responsibility items set out in section 4, the following are deemed as unacceptable IT use and unacceptable behaviours by learners during study and project workshop days and/or using Centre or Trust equipment:

- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Using the internet to send offensive or harassing material to other users
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Hacking into unauthorised areas
- Publishing defamatory and/or knowingly false material about the Centre, Trust or NHS, your colleagues and/or our patients on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Revealing confidential information about the Centre, Trust or NHS in a personal online posting, upload or transmission - including financial information and information relating to our patients, visitors, business plans, policies, staff and/or internal discussions.
- Breaching the General Data Protection Regulation Guidelines and/or the Data Protection Act for information security.

9. Personal Equipment

- 9.1 Personal equipment, including mobile phones, are brought into the Centre at the learners own risk. It remains the responsibility of the learner and the Trust, or Centre, take no liability for it.
- 9.2 Learners should ensure any personal equipment used on Trust premises is PAT tested.
- 9.3 Learner equipment must not interfere with Trust equipment and if requested to cease using it because of interference the learner will do so immediately.
- 9.4 Learners will ensure that personal digital equipment is turned off when left unattended.

