Online Safety Policy

Most recent update: 08 September 2025

Scope

This Online Safety policy covers provision delivered internally by Cheshire West & Chester Council (CW&C)'s Skills and Employment Service and externally by our sub-contracted partners. The policy covers learners and programme participants within classroom and open access settings (for example Skills and Employment Hubs), within council venues and in sub-contracted partner venues. The policy encompasses the use of our Virtual Learning Environment (VLE) as well as the use of the internet, electronic communication and mobile devices. It highlights the need to educate learners about the benefits and risks of using new technology, provides safeguards and raises awareness for users to enable them to control their online experiences.

We recognise that technology is constantly evolving so this policy covers all hardware currently authorised for use within our provision e.g. PCs, laptops, tablets, mobile phones and online learning provision via our VLE. Staff will adhere to the equivalent policy on the Council intranet site.

Purpose

This Online Safety Policy will operate in conjunction with other Skills and Employment (S&E) policies designed to keep our customers safe and free from harm whilst they participate in our services.

Practice

Learners and programme participants will have access to the internet within our venues for research and education purposes as well as job search. We welcome this as a means for improving the IT skills of users, supporting learning through research and securing jobs.

Adult education learners may also occasionally use our Skills and Employment VLE (Moodle). This open-source learning management system has been designed to offer learners remote access to courses and workshops to complement face to face learning. Our VLE has been designed to keep learners safe whilst online and to provide maximum data security.

1. General Internet Usage

Learners and programme participants are encouraged to use the internet for learning and research and will be taught how to evaluate relevant websites and content as part of their course or centre induction. Council and sub-contracted partner learning systems will operate internet filtering software. Network proxy servers are in place to monitor and safeguard learners and programme participants from accessing inappropriate sites; this software is regularly reviewed and monitored to ensure that the filtering is appropriate and suitable for the age ranges of the learners and programme participants using the system. Where access to inappropriate websites takes place, the learner will have their access to the system withdrawn. Staff should report any incidents to their line manager. Any person found to be deliberately re-routing access to avoid these restrictions will also be subject to Council and sub-contracted partner disciplinary proceedings.

The Council and sub-contracted partners' computer systems which are primarily for learning should only be used for this purpose. Any use of the system for private purposes should be within centre guidelines and only outside scheduled class or activity times. Users must not use the systems for personal banking, purchasing or any other commercial purposes.

The Council and sub-contracted partners take reasonable steps to protect users from accidental exposure to explicit material. Any breaches of the policy must be reported to the nearest member of staff.

Our Prevent Duty

Under the Prevent duty, we have a statutory obligation to promote the values we uphold and adhere to in Great Britain. These British values are:

- Democracy
- Rule of law
- Individual liberty
- Mutual tolerance for those with different faiths and beliefs

In upholding these values within our service, we have a duty to take action and report where we identify activity that could contravene and oppose these values through extremist views and/or actions. Extremism can include:

- Right wing extremism
- Religious extremism
- Animal rights extremism
- Other forms of extremism

Online activity is a key area that extremist views could be viewed, circulated and acted upon. It is the responsibility of every staff member to be vigilant regarding accessing extremist views online. Staff must also be aware of the potential for our learners and programme participants to be drawn in or groomed online for extremist purposes.

Internet Usage Rules

- Users must not attempt to access, download or upload information that is obscene, sexually explicit, racist or defamatory, incites or depicts violence, accessed to cause distress to others or describes techniques for criminal or terrorist acts

- Users must not intentionally access or transmit computer viruses or attempt to 'hack' into data that may damage the Council network

- Users must not infringe copyright - this includes unauthorised copying of images from the internet without permission, including the downloading of apps, games, music files etc.

- Users will not use the council systems for gambling under any circumstances

- Users will not use the council systems to access commercial payday loan sites
- Access to sites such as payday lenders will be disabled on council PCs
- It is not permitted to make use of loopholes in internet or website's security systems to access, damage or alter any files held on any computer or website (according to the Computer Misuse Act)
- Users must not knowingly undertake any action that will bring the council into disrepute

2. Email Usage

- Downloading and passing on copyrighted information, or material which may be considered to be violent, obscene, abusive, racist or defamatory will be treated by the Council as gross misconduct. Be aware that such material which may be contained in jokes sent by email can be considered to be harassment. Any person receiving such email should report it to their tutor or staff members
- Users must not knowingly send or receive information that will bring the council into disrepute
- Information sent by email may become subject to the General Data Protection Regulations (GDPR). All users must comply with GDPR where appropriate
- Email must not be used for unsolicited advertising and must not be used for the purposes of private commercial activity
- Users sending email must not flood the network by sending unnecessary information to all users. This uses server space, bandwidth on the network, and may prevent important information getting through. This is particularly important when sending attachment files and documents
- Users will be routinely reminded not to reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission

3. Social Networking And Personal Publishing

- The Council and sub-contracted partners will block or filter access to social networking sites unless approved by tutors or employment mentors in specific areas of the Council for educational or development purposes. In these circumstances, users will be routinely reminded how to use social media sites safely, for example not to put images of family member on a social network site
- Users will be advised never to give out personal details of any kind, which may identify them or their location
- Users must not place personal photos, videos or music on any council network space unless approved by tutors or employment mentors in specific areas of the Council for educational or development purposes
- Learners should be advised on security and encouraged to set secure passwords, deny access to unknown individuals and block unwanted communications. Users should be encouraged to ensure that virtual communications areas are open only to known friends

- Users will be refused access to our IT if it is found that they any communication could be construed as malicious in intent

4. General Use Of Electronic Devices

PCs, laptops, tablets and mini iPads are utilised in our classrooms and support venues. Where possible we also encourage learners to use their mobile phones to take part in MS Teams meetings as part of the blended learning or support approach.

Any individual passwords issued must not be disclosed or shared with others. Computer users should make sure they log off at the end of their session to avoid other users accessing their desktop and private data.

5. Using The CW&C Adult Education Virtual Learning Platform

CW&C provide a Virtual Learning Environment (VLE) for our learners to access provision from a distance as well as our more traditional face to face learning. We provide resources for learners to follow remotely and our tutors mark work submitted online. Safety considerations will be routinely built into all online provision and guidelines will be given at induction, including:

- Clear guidelines on what is appropriate conduct online. As a member of the VLE, they share a digital environment and their behaviour impacts the success of the online adult education community
- Users should keep login details private and ensure that they do not share their account with anyone
- Information about Cyber-bullying and our policy document
- Messages will be visible to council staff and users should not put anything in a message that they would not want anyone else to see
- Tutors and employment mentors will monitor any chat function or message boards to ensure content is appropriate to write online. Learners and programme participants will be reminded that they must not post messages that contain:
  - any offensive, obscene, harmful, threatening, abusive, harassing, slanderous, hate-inciting, racist or criminal content
  - anything that causes embarrassment to CW&C or its customers
  - personal data about another person including names, contact details and sensitive personal data e.g. about another user’s mental or physical health, racial or ethnic origin, religious or other beliefs
- Messages will show who has posted them and learners and programme participants must not pass messages off as being from another person
- Learners and programme participants should understand how to increase the security of their home network by installing anti-virus and anti-malware software

VLE Disclaimers & Responsibilities

- Information provided to learners may contain links to third party websites. CW&C has no control over - and assumes no responsibility for - the content, privacy policies or practices of any third-party websites
- Every learner and programme participant is responsible for the content and data he/she publishes. Users access the VLE and live chat facility at their own risk. To the extent permitted by law, CW&C shall not assume any liability for damage or losses of any kind resulting from the use of the VLE and the live chat tool facility within it. We reserve the right to withdraw content and or information without notice and at our sole discretion
- Learners and programme participants must not enter, publish or transmit content by email or in any other way if this violates the rights of third parties, particularly patents, marks, copyrights, business secrets or other ownership rights
- The VLE and live chat tool must not be used for commercial purposes or to advertise or sell goods

6. Video Conferencing Software

CW&C use MS Teams to deliver online learning using video-conferencing. This software enables a digital face to face element to the learning programme and communication between learners and the tutor. Whilst they are a great way to keep in touch, to safeguard both learners and staff, one-to-one contact is not generally advised. Other safety considerations include:

- Do not put unnecessary personal information in the user profile. For example, try to keep location, phone number and dates of birth private
- The Council will ensure that all software is kept up to date and secure
- Learners to be supported to refuse unwanted requests for contact from other learners outside of the class environment

Breach of any of the above rules is a serious disciplinary offence and may result in the Council taking legal action against the offender

Promotion of this policy

- CW&C staff and sub-contracted partners will include safe online practices within inductions, course delivery and programme activities. In keeping with this policy all tutors and employment mentors will promote up to date online safety messages in all sessions to ensure that learners and programme participants are aware of relevant threats and how best to respond
- Online safety leaflets will be displayed in open access areas
- Posters promoting the online safety policy related to a particular centre (e.g. Skills and Employment Hubs) will be prominently displayed

- Staff will always take action where learners and programme participants disregard or contravene acceptable usage guidelines

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by the appropriate Centre Manager but should be reported to Skills and Employment Designated Safeguarding Lead Officer – Matthew Smith (details below) using the Skills and Employment Incident Report form
- Situations concerning safeguarding and child protection issues (including extremism) will be dealt with according to the Skills and Employment Safeguarding Policy
- Young learners' parents, carers or guardians, will be informed of any breach of procedure and of any complaints

Further information can be found on our website in the following related documents:

- Data Protection and Information Security Policy
- Safeguarding Policy
- Personal Harassment and Bullying Policy

For further information or support on this policy please email Mathew Smith on matthew.smith@cheshirewestandchester.gov.uk