E-SAFETY POLICY

Reviewed by Adam Davies, Quality Manager

Approved by Lynne Whitehouse, Operations Director

Version date: 8/6/22

Review date: 8/6/23 or in line with operating procedure and/or legislative updates/requirements

Person/s responsible: SLT, all management and staff

Signed(author) Adam Davies

Signed

Policy owner

POLICY STATEMENT

The internet is an integral part of 21st century life for education, business and social interaction and Netcom Training has a duty to provide adult learners with quality access as part of their learning experience. The purpose of internet use in Netcom Training is to help raise educational standards, promote learners' achievement, develop learners' internet skills in good internet practice, support the professional work of staff and enhance the organisations management information and business administration systems. Internet use is a part of the curriculum and a necessary learning tool for staff and learners.

This policy has been developed to ensure that all staff at Netcom Training are working together to safeguard and promote the welfare of learners.

AIMS

- To promote the safe and effective use of digital technology to support learning and the smooth running of internal systems;
- To identify simple ways in which e-safety issues can be reported to responsible persons.
- To provide a clear policy and guidelines to enable e-safety to be tackled effectively.
- To put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained through the use of ICT, whilst minimising any associated risks.
- To minimise the potential risk of harm to learners or staff in the following broad areas:

  -Exposure to illegal, inappropriate or harmful material

  -Subjection to harmful online interaction with other users

  -Engagement in behaviour that increases the likelihood of, or causes, harm.

PRINCIPLES

- All staff can recognise and are aware of e-safety issues with regular training and updates;

-E-safety is a priority across all areas of the business

-E-Safety is a safeguarding issue as well as an ICT issue and all staff members have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

The curriculum should ensure varied and regular opportunities to teach learners about e-safety.

PROCESSES

ROLES AND RESPONSIBILITIES

All staff have a role in ensuring safe and purposeful use of the internet and other digital technology and are responsible for such both on the training premises and when supervising online learning and

extension activities. This role will be carried out during lessons where internet and other digital technology is in use and in tutor sessions, other lessons as appropriate and in informal meetings with learners involving their safety and wellbeing.

USING THE INTERNET SAFELY TO ENHANCE LEARNING

- Staff will be made aware of (through CPD and published guidance) and learners via induction and learning sessions in the safe use of the internet.
- Clear boundaries will be set and discussed with staff and learners, for the appropriate use of the internet and digital communications.
- Learners will be developed in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Staff will endeavour to ensure that the use of internet derived materials by staff and by learners complies with copyright law.
- If staff or learners discover an inappropriate site, it must be reported to an e-Safety (Safeguarding) lead via any member of staff.
- Learners will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

USE OF EMAIL

- Learners must be made aware of how they can report abuse and who they should report abuse to.
- Learners and staff should only use approved e-mail accounts.
- Learners will be told to report if they receive offensive or inappropriate e-mail.
- In e-mail communication, learners will be advised not to reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- All staff users will include a signature giving their name, job title and the Netcom Training contact details as per an agreed protocol.
- Staff must not use the Netcom Training email system to promote activity outside of the provision (such as a business interest nor to arrange or discuss social activity)
- The forwarding of chain letters is not permitted.

MANAGING INTERNET ACCESS AND INFORMATION SYSTEM SECURITY

- Netcom Training ICT system security will be reviewed regularly with our ICT support provider.
- The Managing Director and the designated safeguarding lead will receive reports of any concerns about internet or email usage and will act upon these accordingly.
- Virus protection will be installed and updated regularly.

PUBLISHED CONTENT AND THE WEBSITE

- Staff or learner personal contact information will not be published on the website or via social media. The contact details given online will be that of the head office.

PUBLISHING LEARNERS' IMAGES AND WORK

- Photographs that include learners will be selected carefully with due regard to requests for "no photographs" so that images of individual learners cannot be misused.

- No photographs of learners should be taken using staff's own devices.

- Written permission, using the approved permission form will be obtained before learner names, photographs of learners or their work are published on the Netcom Training website or social media platforms of use. This will be renewed annually.

SOCIAL NETWORKING AND PERSONAL PUBLISHING

- Staff will be trained in the safe use of social networking sites, and will develop learners skills in their safe use. Learners will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Learners must be made aware of how they can report abuse using the facilities provided by social media sites.

- Learners should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Learners will be advised through sessions and the wider learning curriculum, be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Learners will be told to only invite known friends and deny access to others.

MANAGING EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment and GDPR compliance will be carried out before use across the provision is allowed.

- The sending of abusive or inappropriate text messages is forbidden in Netcom Training.
- Senior staff are aware that technologies such as mobile phones with wireless internet access can bypass Netcom Training filtering systems and present a new route to undesirable material and communications. Staff will be trained and vigilant to observe/report any suspicious activity.
- Mobile phones belonging to members of staff should not be visible in areas where learners are present.

POLICY DECISIONS

Authorising Internet access

- All staff, including temporary staff and volunteers as well as governors must read and adhere to the IT Security and E- Safety Policy before using any Netcom Training ICT resource, including any laptop issued for professional use and

- Netcom Training will maintain a current record of all staff and learners who are granted access to ICT systems.

ASSESSING RISKS

Netcom Training will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Netcom Training's network. Netcom Training will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken.

MONITORING, ASSESSMENT AND EVALUATION

Information to assist with the monitoring of the policy will be collected in the following ways:

- Staff and learner feedback
- Behaviour incidents and other logs
- Reports to the Advisory Board

The policy and procedures will be reviewed at least annually or in the light of significant changes to processes or legal requirements or policy breaches. Any such changes will be communicated at the earliest opportunity to all relevant staff, learners and other parties that may be affected.