Policy Name	e-Safety Policy	
Policy Reference	NWCS-OP07	
Policy Owner	Paul Sheron	
Latest Review Date	31/01/2023	
Next Review Date	31/01/2024	
Version	**Approved by**	**Summary of changes**
1	PS	

Aim and Purpose of the policy	To ensure that 100% of employed personnel are aware as e-safety policies and procedures that will help **mitigate risk and respond to concerns,** ensuring they have the knowledge to teach learners about e-safety/
Who is this policy for?	This policy relates to all staff employed by NWCS
Key contacts and resources	Key Contacts Head of Centre- Paul Sheron Operational Manager- Karen Luxon Resources -Keeping Children Safe in Education (DfE September 2022)
Relate Policies and Procedures	-Safeguarding Policy -Equality Policy

Aim and Vision

North West Community Services Training Ltd (NWCS) e-Safety policy sets out our commitment to keeping children and young people (as well as staff and volunteers) safe online.

Rationale

North West Community Services Training Ltd (NWCS) recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available means that we are also aware of potential risks and challenges associated with such use. Our approach is to implement safeguards within the centre and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard learners., We will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

Intent

The policy applies to all users OR all learners and staff OR all members of the NWCS community who have access to NWCS IT systems, both on the premises and remotely. Any user of NWCS IT systems must adhere to and sign a hard copy of the acceptable use agreement. The e-Safety Policy applies to all use of the internet and electronic communication devices such as email, mobile phones and social networking sites.

Implementation

There are clear lines of responsibility for e-safety within the centre as detailed within the acceptable user policy and the rules detailed below. The first point of contact should be **Paul Sheron** the e-Safety/Safeguarding Officer. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All teaching staff are required to deliver e-safety awareness sessions to classes. When informed about an e-safety incident, staff members must take particular care to guarantee confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be **their Key Worker/Tutor or Assessor**. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Safeguarding Committee may be asked to intervene with appropriate additional support from external agencies. To make things very clear to all parties, the provider has listed all those persons who have responsibility for safeguarding within their policy.

Below are some examples of roles and responsibilities that may be relevant to NWCS.

<u>e-Safety Lead / Chair of the Safeguarding Committee</u>

Responsible for leading the e-Safety Committee, arranging for staff development and training, recording incidents, reporting any developments & incidents and liaising with the local authority & external agencies to promote e-safety within the provider community.

<u>Learner:</u>

Learners are responsible for using the provider IT systems and mobile devices in accordance with the acceptable use policy, the e-safety rules detailed below which they must agree to and

sign. Learner usage must also comply with the HM Government publication in relation to 'Prevent'. They are expected to seek help and follow procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the provider community. Learners must act safely and responsibly at all times when using the internet and/or mobile technologies.

Staff:

All staff are responsible for using the IT systems and mobile devices in accordance with the acceptable use policy, and the rules detailed below which they must actively promote through embedded good practice. Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times.

All staff should apply relevant college policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the Safeguarding Committee or SMT in their absence without delay.

Security

The provider will do all that it can to make sure the network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of college systems and information. Digital communications, including email and internet postings related to the college will be monitored.

Behaviour

NWCS will ensure that all users of technologies adhere to the standard of behaviour as set out in the acceptable use. The provider will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. Where conduct is found to be unacceptable, the provider will deal with the matter internally. Where conduct is considered illegal, the provider will report the matter to the police.

Communication

NWCS requires all users of IT to adhere to the staff handbook and the acceptable user policy which states clearly when email (apart from work email), mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras may be used during the learning day. Any extension of this policy will require express written permission of **Paul Sheron**. Under no circumstances should staff members liaise via these methods with learners outside of working hours. ***Staff members should also refrain from issuing learners their personal mobile numbers, personal email addresses as a form of communication for any purpose.***

Use of Images and Video

The use of images or photographs is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or learners.

All learners and staff should receive training on the risks in downloading these images as well as posting them online and sharing them with others. There are particular risks where personal images are posted on social networking sites, for example.

NWCS staff will provide information to learners on the appropriate use of social networking. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. No image/photograph should be copied, downloaded, shared or distributed online without permission. Photographs of activities on the college

premises should be considered carefully and have the consent of **Paul Sheron** before being published. Approved photographs should not include names of individuals.

Personal Information
Personal information is information about a particular living person. NWCS collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The provider will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner OR parent OR carer. No personal information can be posted to the college website/without the permission of **Paul Sheron**. Only names and work email addresses of (senior) staff will appear on the provider website.

Staff must keep learners' personal information safe and secure at all times. No personal information of individuals is permitted offsite unless the member of staff has the permission of **Central Administration**. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device.

Education and Training
With the current unlimited nature of internet access, it is impossible for the provider to eliminate all risks for staff and learners. It is our view therefore, that the provider should support staff and learners through training and education. This will provide them with the skills to be able to identify risks independently and manage them effectively.

For learners:
Learners should also know what to do and who to talk to when they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. Information as to this can be found within the departmental Safeguarding policy and highlighted in posters and leaflets around IT areas and work stations.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Incidents and Response
Where an e-safety incident is reported to the centre the matter will be dealt with very seriously. The college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so with their **Key Worker if applicable** or to a **member of the Safeguarding Committee.** Where a member of staff wishes to report an incident, they also contact **a member of the Safeguarding Committee.** Following any incident, the college will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Feedback and Further Information
NWCS welcomes all constructive feedback on this and any other college policy. If you would like further information on e-safety, or wish to send us your comments on our e-Safety Policy, then please contact: **Paul Sheron**

Useful Links for Further Information:

Child Exploitation & Online Protection Centre http://www.ceop.police.uk

Internet Watch Foundation http://mobile.iwf.org.uk

DirectGov-'Staying Safe Online'
http://www.direct.gov.uk/en/YoungPeople/CrimeAndJustice/KeepingSafe/DG_10027670

Get Safe Online http://www.getsafeonline.org

E-Safety Rules & Guidance for using the Internet

- Never share your username and password with others.
- All network and Internet use must be appropriate to your course of study.
- Copyright and intellectual property rights must be respected – always acknowledge where your information came from and quote your sources.
- Always use your work email for work matters. Staff will ONLY use work email addresses when communicating with students.
- Email messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Do not open personal emails or messages, unless you know who they are from.
- You must not forward confidential messages or other sensitive information.
- Users must take care not to reveal personal information through email, personal publishing, social network sites, tweets, blogs or messaging (including text messages).
- Use of social networking sites and chat rooms are not permitted whilst upon the company premises.
- Your use of the I.T. facilities must not harass, harm, offend or insult others, either inside or outside the provider.
- Be aware of the dangers of cyberbullying and always report any suspected cases in confidence to a member of the Safeguarding Committee
- Take care when posting photographs or video clips or yourself and be aware they could be posted by others without your permission, or may be used against you in some way.
- When posting photographs or video clips of others, always ensure you have their permission.
- Anonymous messages and chain letters are not permitted.
- Use of websites for financial gain, gambling, political activity, advertising or downloading music or films for personal use is not permitted.

Impact
It is a requirement that 100% of employed personnel, guests and learners are aware as to the process to adhere to when operating NWCS systems. Young people do not always recognise the inherent dangers of the internet and often do not understand that online behaviour may have offline consequences. Despite this, digital technologies can offer them opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should out-weigh the disadvantages. However, this policy will enable a greater understanding to the extent of the risks the digital world can pose. Subsequently keeping all learners safe.

Definitions
None

Policy Review and Implementation
This policy will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.

This policy is specific to that of NWCS Training Ltd and has been ratified by Head of Centre Paul Sheron

31/01/2023