Online Safety Policy for Students

2024-2025

Contents

1. Introduction

1.1 Cornwall Neighbourhoods for Change (CN4C) has a positive policy of equality and diversity and strives to support students wherever possible. CN4C also has a duty of care to safeguard all its stakeholders including staff, students and visitors and is committed to providing a safe environment for study and work.

1.2 As part of an ongoing commitment to safeguard all its stakeholders the CN4C operates a policy whereby all students must adhere to online safety restrictions.

1.3 CN4C will make every effort to ensure that students are given every opportunityto access online content in order to study, provided it can ensure its safeguarding commitment.

1.4 Computer skills are vital to access employment and life-long learning as ICT is now seen as anessential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings users into contact with a wide variety of influencessome of which may be unsuitable.

1.5 The use of technology has become a significant component of many safeguarding issues suchas child sexual exploitation, Harmful Sexual Behaviour, radicalisation and sexual predation. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm

1.6 These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the online world. Current and emerging technologies in CN4C and more importantly, in many cases used outside of CN4C by students, include (but are not limited to):

- Internet websites
- Virtual Learning Environments
- Instant messaging
- Social networking sites
- E-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites

- Mobile phones with camera and video functionality
- Digital cameras
- Smart phones, iPads and Tablets with e-mail and web applications.

2. Aims of the Policy

2.1 To ensure that all learners at CN4C achieves their full potential safely in an environment free from discrimination.

2.2 To have procedures that take account of an individual's right to education balanced by the risk to CN4C and its wider community.

2.3 To prepare learners for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies.

2.4 To provide guidance on the safe and acceptable use of Online Technologies including social media communications, by learners inside and outside of CN4C.

3. Scope of Policy

3.1 This policy applies to all learners throughout CN4C, irrespective of their method of application or enrolment or their type of study including those on further education, higher education (including programmes awarded by partner institutions), studying either full-time or part-time, whilst attending a CN4C course.

3.2 The policy also applies to use of social media and other communication platforms inside and outside CN4C.

4. Online Safety

4.1 CN4C has an Online Safety policy to protect learners. The policy recognises that Online Safety encompasses not only the Internet but any type of electronic communication, such as mobile phones and devices with wireless technology.

4.2 It is important for all learners to understand the Internet is an unmanaged, open communications channel. Anyone can send messages, discuss ideas and publish material with no restriction. These features of the Internet make it an invaluable resource used by millions of people every day - however not all information is correct, accurate or valid.

4.3 Students should be aware that publishing personal information could compromise your security and that of others.

4.4 CN4C will continually make it clear to all learners that the use of CN4C equipment for inappropriate reasons is unacceptable. CN4C will take reasonable actions and measures to protect all its users, including (although not limited to) disciplinary action. Please see CN4C's Student Behaviour and Values Policy. Learners must report to a tutor or a safeguarding officer if a member of staff attempts to communicate with them via social media.

5. Safeguarding

5.1 Radicalisation

5.1.1 Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism which are illegal. Learners must report to any member of staff if they view any extremist or radical views expressed online. Tutors will then follow CN4C's Safeguarding procedures.

5.1.2 There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer.

5.1.3 The Internet and the use of social media has become a major factor in the radicalisation of young people.

5.2 Child Sexual Exploitation

5.2.1 Child Sexual Exploitation (CSE) may involve utilising the Internet and Social Media to identify potential victims or as a tool to coerce and blackmail young people into performing sexual acts, both on and offline. (HSB)

5.2.2 Means of accessing the Internet may also be provided to young people as a "gift" by perpetrators such as in the form of new mobile phones and devices. In some cases, CSE / HSB can take place entirely online such as young people being coerced into performing sexual acts via webcam/Social Media and therefore may not always result in a physical meeting between young person and the offender.

5.2.3 **Sexual abuse: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether the young person is aware of what is happening. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other young people.**

5.3 Youth Produced Sexual Imagery and Sharing of Inappropriate Imagery

5.3.1 **Youth Produced Sexual Imagery (YPSI – formerly known as 'Sexting') can be defined as'an increasingly common activity among young people, where they share inappropriate or explicit images online'. This can include sharing indecent images of themselves or others via mobile phones, webcams, social media and instant messaging.**

5.3.2 **Although viewed by many young people as a 'normal' or 'mundane' activity and part of 'flirting', YPSI can be seen as harmless; but creating or sharing explicit images of a child is illegal, even if the person doing it is a child.**

5.3.3 **A young person is breaking the law if they:**

- **take an explicit photo or video of themselves or a friend.**
- **share an explicit image or video of a child, even if it's shared between children ofthe same age;**
- **possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.**

6. Social media

6.1 Social media is a useful tool; the CN4C understands that learners communicate and collaborate via sites and apps on a regular basis and it is to be noted that there are merits to this. Learners should familiarise themselves with and adhere to guidelinesand etiquette as found in Appendix 2 of this document.

6.2 Unfortunately, there are also risks attached to the use of social media. Learners must immediately tell their tutor or safeguarding staff if they receive offensive or inappropriate messages whilst they are studying at CN4C. This includes messages sent to personal mobile phones or devices.

7. Accessing the Internet CN4C premises: Monitoring & Filtering

7.1 The Internet is available at all CN4C buildings to help students with their studies. Whilst it is essential that appropriate filters and monitoring processes are in place, CN4C recognises that 'over blocking' does not lead to reasonable

restrictions and does not replace what young people and adults are taught with regards to online safety and safeguarding. Learners must immediately tell a lecturer or safeguarding officer if they think their network account has been tampered with.

7.2 Uploading and/or circulation of derogatory or defamatory comments and/or images about Cn4C and/or its staff and/or learners to any internet service (websites, social media, etc) is not permitted. Abuse of the Internet facilities will be seen as improper use of CN4C equipment and will lead to disciplinary procedures (see Appendix 1).

7.3 The V Learning Net Consortium has implemented content filters to prohibit access to the categories listed below. Any student found attempting to access inappropriate or harmful material will besubject to the CN4C procedures. This list is updated regularly:

- **Discrimination: Promotes the unjust or prejudicial treatment of people on thegrounds of race, religion, age or sex**
- **Drugs/Substance abuse: Displays or promotes the illegal use of drugs orsubstances**
- **Extremism: Promotes terrorism and terrorist ideologies, violence or intolerance**
- **Malware/Hacking: Promotes the compromising of systems including anonymousbrowsing and other filter bypass tools as well as sites hosting malicious content**
- **Pornography: displays sexual acts or explicit images**
- **Piracy and copyright theft: Includes illegal provision of copyrighted material**
- **Self-Harm: Promotes or displays deliberate self-harm (including suicide andeating disorders)**
- **Violence: Displays or promotes the use of physical force intended to hurt or kill**

N.B. This list is not exhaustive.

8. Data Protection

8.1 CN4C will comply with the Data Protection Act 2018 and GDPR by ensuring that personal data is:

- **Collected and processed lawfully, fairly and transparently for only specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest,research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.**

- **Adequate, updated and relevant and not excessive for the purposes it was collected.**

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisationalmeasures. Including not being transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal datamay be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

9. Confidentiality

9.1 The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR) replaced the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal datafrom 25 May 2018.

9.2 These are not only restrictions on disclosure of information about CN4C, they are bound by a common law duty of confidentiality. This duty prevents CN4

from releasing information about learners without their consent. This dutyapplies to manual records as well as information held on computers.

9.3 Information which must be treated as confidential includes the names and addresses of learners and any other information about them which is not publicly known aka "personal data". Accordingly, to ensure that we do not breach ourduty, no information, even if it only exists in printed form, should be disclosed unless all the relevant procedures have been followed.

9.4 Under UK GDPR, anyone is entitled to make a Subject Access Request, to gain a copy of the data relating to that individual by an organisation.

10. Raising Awareness

10.1 Online safety awareness is delivered throughout the year, to all learners in a range ofways that are relevant to the courses being delivered.

10.2 Learners can access advice in regards to their online safety settings by speaking to their tutor. Further guidance can be found from the websites listed below.

10.3 Students are expected to adopt an attitude of 'collective responsibility' towards onlinesafety by encouraging others to stay safe and report any concerns to a member of CN4C staff.

11. Other Relevant Procedures

11.1 Related CN4C policies and procedures include:

- Computer Security Policy
- CN4C Staff Behaviour Policy
- Student Behaviour and Values Policy
- Safeguarding Policy and Procedures
- Equality and Diversity Policy
- Data Protection Policy
- Anti-bullying Policy

Appendix 1

Activity deemed inappropriate which may lead to disciplinary proceedings under CN4C Safeguarding procedures

Gross Misconduct

- **Bullying, including cyber-bullying i.e. any form of bullying which takes place online orthrough smartphones and tablets**
- **Wilful damage to CN4C property including;**
    - **Malicious attacks on the network.**
    - **Distributing malware.**
    - **Physical Damage to computer equipment around CN4C i.e re-arrangingletters on keyboards, graffiti or Damage to computer screens, etc.**
- **Downloading, storing, transmitting or viewing pornographic or offensive material.**
- **Capturing, possessing and/or circulating inappropriate material.**
- **Inciting others to carry out acts of misconduct or gross misconduct.**
- **Spreading or publishing radicalised / intolerant views or materials.**
- **Violating any part of the Computer Misuse Act 1990.**

Misconduct

- **Misuse of the computer network i.e. chat lines/social networking sites, use ofanother learners password, inappropriate use of the internet**
- **Failure to return equipment**

N.B. This list is not exhaustive

Appendix 2

We must all adhere to the following guidelines when accessing social media sites and apps

- **Use of sexually explicit language or viewing, creation or sharing of sexually explicitimagery is not permitted nor advised from a safeguarding perspective.**
- **Verbally abusive, intolerant or threatening language is strictly prohibited.**
- **Use of racist or extremist language which would directly contravene British orCN4C values, is not permitted.**
- **Use of social media for radicalisation or the expression of extremist views is notpermitted.**
- **Communication with staff unless on a CN4C controlled platform is not permitted. Any such communication instigated by staff members to a learner's personal socialmedia must be reported to safeguarding team.**

Please be mindful of the following when using social media:

- **Avoid posting anything on social media that you wouldn't want others to see. Remember what you post could impact on your future career.**
- **Don't be pressured into doing anything inappropriate on social media like posting photos or videos. You must report any requests you receive through social media topost sexually explicit or offensive imagery online, to your tutor or safeguarding staff.**
- **Beware of accepting people as friends or engaging in conversations on social mediaif you don't know the people you are communicating with**
- **Exercise caution when accessing personal social media platforms in a publicenvironment, e.g. a classroom or library.**
- **Set any personal social media profiles to "private" to ensure control over who is ableto access / view your information.**
- **Ensure your behaviour online cannot be conceived as detrimental to CN4C orits reputation.**
- **Be security conscious and take steps to protect yourself from identity theft, this canbe achieved by restricting the amount of personal information given out on Social Media platforms. These platforms allow people to post detailed personal information such as date of birth, place**

of birth and favourite football team. These are often the answers to security questions and parts of passwords.

- **Change your social media password often..**