Norman Mackie & Associates LTD

Trading As

Works 4 U Support Services

Online Safety Policy

HEAD OFFICE – STALYBRIDGE:

Works4U, The Peacock, Ambleside, Stalybridge, Cheshire, SK15 1EB
Telephone: 0161 303 1069 Email: works4u@normanmackie.com Web: www.works4u.org.uk

safeguarding@normanmackie.com

Last updated September 2021
Note any questions or comments relating to these policies should be addressed to:
Wendy Mackie – Managing Director – Works4U Support Services – 0161 303 1069

Contents

1. Introduction

1.1 Works4U has a positive policy of equality and diversity and strives to support learners where ever possible. Works4U also has a duty of care to safeguard all of its stakeholders including staff, learners and visitors and is committed to providing a safe environment for study and work.

1.2 Works4U will make every effort to ensure that learners are given every opportunity to access online content in order to study, provided it can ensure its safeguarding commitment to the whole Works4U community.

1.3 Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential 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 staff and students into contact with a wide variety of influences some of which may be unsuitable.

1.4 The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation; 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 Works4U environment. Current and emerging technologies in Works4U and more importantly, in many cases used outside Works4U by students, include (but are not limited to):

- Internet websites
- 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 everyone who works and learns at Works4U 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 Works4U 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 Works4U.

3. Scope of Policy

3.1 This policy applies to all of our learners, irrespective of their method of application their type of study including school, studying either full-time or part-time.
3.2 This policy will apply to all Works4U sites and all venues and programmes, regardless of location.
3.3 Any risks identified could relate to information / evidence arising prior to or at the time of enrolment, or arising post enrolment whilst studying at Works4U.
3.4 The policy also applies to use of social media and other communication platforms inside and outside of Works4U.

4. Online Safety

4.1 Works4U has an Online Safety policy to protect students, staff and visitors. 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.
4.3 Students should be aware that publishing personal information could compromise your security and that of others. The 2018 revisions to the DfE statutory guidance 'Keeping Children Safe In Education' requires those working in education to act as follows:

"Section 35. All school and college staff should be aware that **abuse, neglect and safeguarding issues are rarely standalone events** that can be covered by one definition or label. In most cases, multiple issues will overlap with one another.

Section 36. **Abuse**: a form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others (e.g. via the internet). They may be abused by an adult or adults or by another child or children (peer on peer abuse).

Section 38. **Emotional abuse**: the persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development, It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying)"

4.4 Works4U will continually make it clear to all learners, staff and visitors that the use of Works4U equipment for inappropriate reasons is unacceptable. Works4U will take reasonable actions and measures to protect all its users, including (although not limited to) disciplinary action. Students

must report to a member of staff or a safeguarding officer – **(Mark Hyde)** 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. Learners must report to any member of staff if they view any extremist or radical views expressed online. Staff should report any concerns immediately to a member of the safeguarding team.

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 in particular has become a major factor in the radicalisation of young people.

5.1.4 *"Radicalised students can also act as a focal point for further radicalisation through personal contact with fellow students and through their social media activity. Where radicalisation happens off campus, the student concerned may well share his or her issues with other students. Changes in behaviour and outlook may be visible to staff. This guidance therefore addresses the need for institutions in receipt of public funding to self-assess and identify the level of risk, ensure all staff have access to training, and that there is welfare support for students and effective IT policies in place which ensure that these signs can be recognised and responded to appropriately".*

"Institutions must have clear policies in place for students and staff using IT equipment to research terrorism and counter terrorism in the course of their learning". (Prevent Duty Guidance: for further education institutions in England and Wales 2015)

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 children into performing sexual acts, both on and offline.

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

5.2.3 *"Section 29 - Sexual abuse: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing, and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. The*

sexual abuse of children by other children is a specific safeguarding issue (also known as peer on peer abuse) in education and all staff should be aware of it and of their school or colleges policy and procedures for dealing with it,"

(Keeping Children Safe In Education, September 2021, section 29)

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 children and 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.

"Section 31 - All staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking and or alcohol misuse, deliberately missing education and consensual and non-consensual sharing of nudes and semi-nudes images and/or videos9 can be signs that children are at risk."

(Keeping Children Safe In Education, September 2021, section 31)

5.3.3 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. 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 of the 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.

5.4. Social media

5.4.1 Social media is a useful tool; Works4U understand that or 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 guidelines and etiquette as found in Appendix 2 of this document.

5.4.2 Unfortunately, there are also risks attached to the use of social media; everyone at the College is expected to use it responsibly, inside and outside of Woks4U premises (This includes all Works4U sites). **Students must** immediately tell their key worker or safeguarding staff if they receive offensive or inappropriate messages whilst they are a student at Works4U. This includes messages sent to personal mobile phones or devices.

7. Accessing the Internet on College premises: Monitoring & Filtering

7.1 The Internet is available on all Works4U systems to help learners with their studies. Whilst it is essential that appropriate filters and monitoring processes are in place, Works4U recognises that 'over blocking' does not lead to reasonable restrictions and does not replace what young people are taught with regards to online safety and safeguarding. Students must immediately tell a member of staff or safeguarding officer if they think their network account has been tampered with.

7.2 The laptop devices come with web-filtering service called Cisco Umbrella installed. This blocks a range of illegal and inappropriate content and limits searching to the 'Safe Search' provided by popular search engines.
The Web-filtering service is strict. We have attempted to balance the needs of all user groups so that it is suitable for the full range of users from young children to care leavers.
The first time the device connects to a new network, there will be a short delay before the content filtering starts to work. This usually takes less than 15 seconds but could take up to 2.5 minutes. During this time, users may be able to access any website without restriction while Cisco Umbrella registers the new device and checks network posts. DfE is working with Cisco to reduce this delay. Any updates made to support this will be deployed to the devices automatically.

8. Raising Awareness

8.1 Online safety awareness is delivered throughout the year, to all students in a range of ways such as sessions which focus on Online Reputation, Exploitation, Online Gaming and Sleep Awareness. Targeted events such as 'Safer Internet Week' and 'Stay Safe Week' are promoted at a cross-college level with a range of activities, information and external professionals providing advice and guidance to both students and staff.
8.3 Students are expected to adopt an attitude of 'collective responsibility' towards online safety by encouraging others to stay safe and report any concerns to a member of Works4U staff.
8.4 Regular training is provided for all staff in regards to online safety, safeguarding, sexual and criminal exploitation and radicalisation though our training platform National on Safety & High Speed Training.

12. Relevant Sources of Information

12.1 Relevant documents include:
- DfES 'Keeping Children Safe in Education' (September 2021)

- Working Together to Safeguard Children - A guide to inter-agency working to safeguard and promote the welfare of children (July 2018)

- UKCCIS 'YPSI in Schools and Colleges' (updated 2020)

- HM Government 'Prevent Duty Guidance: for further education institutions in England and Wales '(Updated April 2021)

- South West Grid for Learning 'So You Got Naked Online?' https://swgfl.org.uk/assets/documents/so-you-got-naked-online.pdf

- NICE 'Harmful Sexual Behaviour Amongst Children and Young People' (Sept 2016)

12.2 Useful websites include:
- Child Exploitation and Online Protection Centre http://www.ceop.police.uk/

- UK Safer Internet Centre http://www.saferinternet.org.uk/

- CEOP's Think You Know http://www.thinkuknow.co.uk/

- Safer Internet Centre Social Network Checklists www.saferinternet.org.uk/checklists

- Get It Right From a Genuine Site http://www.getitrightfromagenuinesite.org/

- Net Aware http://www.net-aware.org.uk/

- Internet Watch Foundation http://www.iwf.org.uk/

Appendix 1

Activity deemed inappropriate which may lead to disciplinary proceedings under Works4U (Code of Conduct) procedure

Gross Misconduct

- Bullying, including cyber-bullying i.e. any form of bullying which takes place online or through smartphones and tablets

- Wilful damage to College property including;

- Malicious attacks on the network.

- Distributing malware.

- Physical Damage to computer equipment around college i.e re-arranging letters 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.

- Bringing the College into disrepute. - 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 of another students 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 explicit imagery 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 or College values, is not permitted.

• Use of social media for radicalisation or the expression of extremist views is not permitted.

• Communication with staff unless on a College controlled platform is not permitted. Any such communication instigated by staff members to a student's personal social media 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 to post sexually explicit or offensive imagery online, to your tutor or safeguarding staff.

• Beware of accepting people as friends or engaging in conversations on social media if you don't know the people you are communicating with

• Exercise caution when accessing personal social media platforms in a public environment, e.g. a classroom or library. • Set any personal social media profiles to "private" to ensure control over who is able to access / view your information.

• Ensure your behaviour online cannot be conceived as detrimental to Works4U or its reputation.

• Be security conscious and take steps to protect yourself from identity theft, this can be 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.