WORKS 4 U

Online Safety Policy

Version 3.0
Updated: 04.09.2025

1. Introduction

1.1 Works4U promotes equality, diversity and inclusion and is committed to safeguarding all learners, staff and visitors. Works4U aims to provide a safe, supportive learning and working environment.

1.2 Works4U will ensure learners can safely access online content necessary for their studies while upholding safeguarding responsibilities across the organisation.

1.3 Digital skills are essential for employment and lifelong learning. However, online technologies also introduce risks, particularly for vulnerable groups. Internet use across society means learners and staff may encounter content and influences that are inappropriate or harmful.

1.4 Technology is a significant factor in safeguarding concerns, including child sexual exploitation, radicalisation, criminal exploitation, bullying, and sexual predation. Online safety risks fall into three categories:

- **Content:** exposure to illegal, harmful or inappropriate material.
- **Contact:** harmful interactions with others.
- **Conduct:** personal behaviour online that increases the risk of harm.

1.5 New and emerging technologies used by students in and outside Works4U include (but are not limited to): websites, instant messaging, social media, email, blogs, video platforms, gaming, live streaming, smartphones, tablets, cameras, and other internet-enabled devices.

2. Aims of the Policy

2.1 To ensure all members of the Works4U community can achieve their full potential in a safe and discrimination-free environment.

2.2 To set out clear procedures balancing learners' rights to education with safeguarding responsibilities.

2.3 To prepare learners for their future by developing safe and appropriate digital literacy and ICT skills.

2.4 To provide clear guidance on safe use of online technologies and social media, in and outside Works4U.

3. Scope of Policy

3.1 This policy applies to all learners, regardless of programme, location, age or mode of study.

3.2 This policy applies across all Works4U sites, off-site venues, and online learning platforms.

3.3 Identified risks may arise before enrolment, at enrolment, or during a learner's time at Works4U.

3.4 The policy applies to all use of social media and digital communication linked to Works4U activities.

4. Online Safety

4.1 Works4U's Online Safety Policy covers all digital communication technologies including internet, email, social media, mobile devices, cloud services and networked systems.

4.2 Learners should be aware that the Internet is an open communications platform. Anyone may publish or share information, and therefore not all online content is accurate, appropriate or safe.

4.3 Learners must understand that sharing personal information can threaten personal safety and the safeguarding of others.

Keeping Children Safe in Education states that staff must understand that:

- Safeguarding issues are often complex and overlapping.
- Abuse may occur online or be facilitated via online means.
- Peer-on-peer abuse, including online harassment and harmful sexual behaviour, must be recognised and addressed.

4.4 Inappropriate use of Works4U equipment or networks is unacceptable. Disciplinary and safeguarding actions may be taken where necessary. Learners must report any communication from staff to personal social media accounts immediately to the Designated Safeguarding Lead (DSL), **Mark Hyde** and the E-Safety Lead – **James Mackie**

5. Safeguarding

5.1 Radicalisation

5.1.1 Radicalisation is the process through which individuals come to support extremist ideologies, including terrorism. Learners must report any online extremist content encountered.

5.1.2 Vulnerability factors vary and may include social, emotional or personal influences. Radicalisation often occurs through online platforms.

5.1.3 Social media plays a major role in radicalisation of young people.

5.1.4 Works4U follows the **Prevent Duty guidance** and ensures:

- Risk assessment procedures are in place.
- Staff receive training.
- Safe and appropriate IT filtering and monitoring are active.
- Welfare support is available.
- Research into terrorism or extremism for academic purposes follows strict guidelines.

5.2 Child Sexual Exploitation (CSE)

5.2.1 CSE may involve grooming or coercion online, including via social media, messaging apps and live streaming.

5.2.2 Devices or data may be used as “gifts” by perpetrators. CSE may occur entirely online without physical contact.

5.2.3 KCSIE 2024 defines sexual abuse as including both physical and non-contact activities, including the creation or sharing of sexual images. Abuse can occur online or offline and may be committed by adults or peers.

5.3 Youth Produced Sexual Imagery (YPSI)

5.3.1 YPSI includes creating, possessing or sharing sexual images involving children (under 18), including self-generated content.

5.3.2 KCSIE highlights that consensual or non-consensual sharing of nudes or semi-nude imagery is a safeguarding issue.

5.3.3 Creating or sharing indecent images of children is illegal, even if all parties are minors. Breaking the law includes:

- Taking an explicit image.
- Sharing it.
- Possessing it.

5.4 Social Media

5.4.1 Works4U recognises that learners use social media widely. Guidance and etiquette expectations are outlined in Appendix 2.

5.4.2 Learners must report offensive, harmful or inappropriate messages received online to staff or safeguarding immediately.

---

6. Accessing the Internet on Works4U Premises: Monitoring & Filtering

6.1 Works4U provides internet access for educational purposes and maintains robust but proportionate filtering and monitoring to uphold safety without excessive restriction.

6.2 Works4U devices are managed by **Inology IT and are compliant with Microsoft Cyber Essentials** - blocking illegal or harmful content and enabling safe search features.

6.3 Brief delays may occur when devices connect to new networks. Users may temporarily access unrestricted content until the filter activates.

---

7. Raising Awareness

7.1 Online safety awareness is provided throughout the year through sessions on reputation, exploitation, gaming safety, digital wellbeing, and more.

7.2 Works4U promotes national awareness initiatives such as **Safer Internet Week**, with activities, guest speakers and information campaigns.

7.3 Learners are encouraged to take collective responsibility for online safety by supporting peers and reporting concerns.

7.4 Staff receive regular safeguarding and online safety training via National Online Safety and High Speed Training platforms.

8. Relevant Sources of Information

- Keeping Children Safe in
- Working Together to Safeguard Children
- UKCIS Guidance on Sharing Nudes and Semi-Nudes
- Prevent Duty Guidance
- NSPCC & CEOP resources

Useful websites:

- CEOP: www.ceop.police.uk
- UK Safer Internet Centre
- ThinkUKnow
- Internet Watch Foundation

Appendix 1 – Examples of Inappropriate Activity

Gross Misconduct

- Cyberbullying.
- Damage to IT systems or equipment.
- Distribution of malware.
- Accessing, sharing or storing pornographic, illegal or harmful content.
- Sharing inappropriate images.
- Bringing Works4U into disrepute.
- Promoting extremist or discriminatory content.
- Breaching the Computer Misuse Act 1990.

Misconduct

- Misuse of networks or social media.
- Using another person's login details.
- Failure to return Works4U devices.

This list is not exhaustive.

Appendix 2 – Social Media Guidance

Prohibited Behaviour:

- Posting or viewing sexually explicit content.
- Abusive, discriminatory or threatening language.
- Posting extremist or radicalised material.
- Communicating with staff outside approved platforms.

Guidance for Learners:

- Think before you post—online actions affect future opportunities.
- Do not feel pressured into sharing images.
- Be cautious when accepting contacts.
- Keep accounts private.
- Protect personal information.
- Change passwords frequently.
- Avoid content that could damage Works4U's reputation.