Online Safety Policy

Online safety policy statement

PQMS Training is committed to ensuring that all our staff & learners are safe online and are provided with the correct guidance and procedure for doing this, and to ensure Safeguarding against these risks is not just an ICT responsibility; it is everyone's responsibility and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable, as outlined in this policy.

This policy has been created in line with the statutory guidance document **Keeping Children Safe in Education, 2023.**

Aims

The aim of promoting online safety is to protect young people from the adverse consequences of access or use of electronic media, including from bullying, inappropriate sexualised behaviour, or exploitation. Many of these risks reflect situations in the non-digital off-line world. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the skills and confidence to face and address these risks.

The main areas of risk for PQMS Training as a learning provider can be summarised as follows:

Content:

- Exposure to illegal, inappropriate, or harmful material, including online pornography, ignoring age ratings in games (exposure to violence and inappropriate language)
- Lifestyle websites, for example mental health/self-harm/suicide sites
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact:

- Being subjected to harmful online interaction with other users
- Grooming
- Cyber-bullying in all forms
- Extremism and radicalisation
- Identity theft and sharing passwords.

Conduct:

- Personal online behaviour that increases the likelihood of, or causes, harm.
- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation
- Health and well-being - amount of time spent online (socialising, watching video or gaming)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (no thought or consideration for intellectual property and ownership – such as music and film).

Communication

The online safety policy will be communicated to staff and learners in the following ways:

- Policy to be posted on the website and in reception areas.
- Policy to be added to myconcern for all staff to read and acknowledge as read.
- Acceptable use agreements to be issued to learners, usually on enrolment.
- Acceptable use agreements to be held on the e-portfolio for learners.
- All learners and trainers will be provided with online safety training.

Handling complaints

- PQMS Training will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a PQMS Training computer or mobile device.
- Staff and learners are given information about actions to be taken in the event of a complaint or breach of this policy.

These include:

  - Interview with DSL and /or CEO
  - informing parents/ carers.
  - referral to Local Authority, Children's Social Care and/or police.

- The DSL acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the CEO.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy; Complaints and/or allegations related to child protection are dealt with in accordance with the PQMS Training and Local Authority child protection procedures:
- All complaints will be dealt with in accordance with our complaints and appeals procedure.

Review and Monitoring

The online safety policy is referenced from within other PQMS Training policies:

- Cyberbullying policy,
- Safeguarding and child protection policy,
- Anti-Bullying and harassment policy,
- Learner behaviour policy,
- Staff behaviour code of conduct policy

The online safety policy will be reviewed annually or when any significant changes occur regarding the use of technologies within PQMS Training.

Online Safety – roles and responsibilities

The DSL will have responsibility for Online Safety. It is crucial that they develop and maintain an online safety culture within PQMS Training.

The responsibilities of this role are to:

a. Develop an online safety culture at PQMS Training.

b. Be the named point of contact on all online safety issues.

c. Ensure online safety is included as part of the induction procedures, and all staff and volunteers receive a copy of the Acceptable Use of technology policy and staff mark as read on Myconcern.

d. Monitor online safety, such as:

    1. Ensuring the technology infrastructure provides a safe and secure environment for learners and staff, for example by ensuring web address filters and other security management software is in place.

e. Reporting on online safety issues to the DSL, CEO, Head of apprenticeships and Governors

f. Ensure that all learners, staff, volunteers, and management/Governor members know what to do if they are concerned about an online safety issue.

g. Keep abreast of developing online safety issues via attendance at relevant training sessions, conferences or seminars, and recommended websites such as:

    a. http://www.saferinternet.org.uk/

    b. http://www.thinkuknow.co.uk

    c. http://www.ceop.police.uk

h. Ensure that online safety is embedded within continuing professional development (CPD) for staff and volunteers, and co-ordinate training as appropriate.

i. Ensure that online safety is embedded across all activities as appropriate.

j. Ensure that online safety is promoted to Learners, parents/carers and others whilst at PQMS Training, the home and the community.

k. Review and update online safety policies and procedures on a regular basis and after an incident.

The curriculum

Learners' online safety PQMS Training:

- Has clear, progressive online safety sessions embedded as part of the apprenticeship programme. This covers a range of skills and behaviours appropriate to the students' age and experience, including how:
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy.
    - To be aware that the author of a web site, blog or post may have a particular bias or purpose, and to develop skills to recognise what that may be.
    - To understand how search engines work and to understand that this affects the results they see at the top of the search results.
    - To demonstrate polite and acceptable behaviour when using software services in an online environment
    - To understand why they must not upload pictures or videos of others without their permission.

  - To know not to download any files – such as video or music files - without permission from the copyright holder.
  - To have strategies for dealing with receipt of inappropriate material.
  - To understand why and how some people will 'groom' young people for criminal, anti-social or sexual purposes.
  - To understand the impact of cyberbullying, sexting, and trolling, and know how to seek help if they are affected by any form of online bullying.
  - To know how to report any abuse and how to seek help if they experience problems when using internet-connected technologies, i.e., parent or carer, tutor or trusted staff member, or an organisation such as ChildLine or the 'Click CEOP' button.
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind learners about their responsibilities through an end-user Acceptable Use of technology policy, which every student will sign/will be displayed throughout the center.
- Ensure staff will demonstrate safe and responsible behaviour in their own use of technology during delivery sessions.
- Ensures that when copying content from the web, staff and learners understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright and intellectual property rights.

Staff Training

- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity of that data requires data protection.
- Make online safety training available to staff on a yearly basis.
- Provides, as part of the induction process, all new staff (including those on an apprenticeship, and work experience) with information and guidance on the online safety policy and PQMS Training's Acceptable Use of technology policies.

Parent Awareness

PQMS Training:

- Provides advice and guidance for parents, including having the policy on the website.

Definitions

What do we mean by 'online'?

When we refer to being online, we include being connected to the internet or communicating through a wide range of devices or technologies, such as computers, laptops, mobile phones, tablet computers, hand-held devices, and games consoles.

PQMS Training

The Training Provider

Parent/carer

The term parent/carer refers to any individual who has parental responsibility for a child or has care for a child (Learners).

DSL

Designated Safeguarding Lead

Use of ICT equipment

Where Learners are allowed free access to browse the internet, e.g., in break time staff must be vigilant in monitoring the content of the websites the young people visit.

Staff who use the PQMS Training's ICT and communications systems:

a. Must abide by PQMS Training's Acceptable Use of technology policy
b. Must use the systems responsibly and keep them safe.
c. Must maintain safe professional boundaries. This includes not giving their personal email address to learners or befriending learners on social network sites, such as Facebook or Instagram.
d. Will have clearly defined access rights to PQMS Training ICT systems. Details of the access rights available to groups of users will be recorded and maintained by Data Productions, and will be reviewed, at least annually, by the CEO.
e. Must treat as confidential any passwords provided to allow access to ICT equipment.
f. Must ensure integrity of passwords. Network user account passwords should be strong (mixture of letters, number and characters) and be changed periodically, e.g., monthly. If a password is compromised, it must be changed as soon as possible and no longer than within 24 hours.
g. Must not install software on the PQMS Training equipment, including apps, freeware, and shareware.
h. Must not use personal devices (e.g., USB memory sticks) to upload or download material onto PQMS Training network or website, or any ICT device.
i. Agree any use of cloud storage systems (e.g., Dropbox, Google Drive, etc.) will be approved by the CEO.
j. Must comply with any ICT security procedures governing the use of systems in PQMS Training, including anti-virus measures.
k. Must report known breaches of this policy to the DSL, including any inappropriate images, messages or other material which may be discovered on PQMS Training's ICT systems.
l. Must ensure that the systems are used in compliance with this online safety policy.
m. Will be provided with online safety training.
n. Understand that system use, including but not limited to internet usage and system logs may be monitored.

This policy will be made available to all our staff and any breaches of the policy will result in appropriate disciplinary action. All staff are responsible for ensuring that the website and social media platforms have appropriate content posted and should report to the designated person if they find this is not the case. Staff should not communicate or be 'followed' by any of their learners through social media platforms or through any private accounts. Staff should always remain professional and avoid the use of emojis or symbols such as ‘kisses’ (X’s) with learners. Any disclosures of abuse reported through social media should be dealt with in the same way as a face-to-face disclosure, and the relevant action taken. Smartphone users should respect the private lives of others and not take or distribute pictures of other people if it could invade their privacy. Staff and learners must not engage in ‘sexting’ or send pictures to anyone that are obscene, indecent, or menacing.

Online safety and use of digital devices

At all times, staff, learners, and volunteers will treat others with respect and will not undertake any actions that may bring PQMS Training into disrepute.

Mobile phones, tablets and other digital devices can present several problems when not used appropriately.

a. Mobile/smartphones, tablets and other personal devices can allow wireless and 3/4/5G internet access via alternative ISPs and thereby bypass the PQMS Training’s security settings and filtering.

b. Mobile/smartphones with integrated cameras could lead to child protection, bullying and data protection issues, regarding inappropriate capture, use or distribution of images of learners or staff.

Equipment

PQMS Training is responsible for ensuring that the network infrastructure, computer equipment and internet provision is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. It will also be necessary to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

All computer equipment is installed professionally and meets current health and safety standards. Equipment is maintained to ensure health and safety standards are followed.

Internet access

There will be situations when learners will need to research topics that would normally result in internet searches being blocked, e.g. racism; drug use; discrimination; freedom of speech, etc. When such a situation is anticipated to arise, staff can request that the Data Productions temporarily relax the standard filtering regime for the defined period of study only. Any request to do so must be requested in writing, with clear reasons for the need, and be authorised by the CEO.

Learners must be taught to acknowledge any source of information they cite or use, and to respect copyright when using material accessed on the internet.

Email

PQMS Training uses Office 365 for emails which includes online protection to detect and block viruses, spam, phishing, Trojan, and other malicious message types.

All staff use standard PQMS Training -issued email addresses.

a. Staff and volunteers will use only a PQMS Training email account for their professional use.

b. All digital communication between staff and learners and parents/carers (email, Messaging) must be professional in tone and content.

c. Learners should be taught about email safety issues, such as the risks attached to the sharing or revealing of personal and private details and opening attachments. They should also be taught strategies to deal with inappropriate communication and be reminded of the need to write emails clearly and correctly and not include any unsuitable, illegal, or abusive material.

d. Staff, volunteers, Governors, and all those connected professionally with PQMS Training will not send material that is illegal, obscene, upsetting, or defamatory, or that is intended to annoy or intimidate another person. Should such content be received, it must not be forwarded to anyone, and must be reported to the DSL, who will take appropriate action.
e. Users should not attempt to send any emails known to contain viruses or be considered spam or phishing, Trojan and other malicious attachments are a danger to PQMS Training systems.
f. Users should be aware that email communications may be monitored.

Data security

Refer to GDPR Data Protection Policy.

Mobile phones

a. Staff must take responsibility for their personal mobile phone when they are working with learners. These conditions also apply to volunteers.

   .

b. Staff are not permitted to use their own personal phones or devices for contacting learners and their families within or outside of PQMS Training in a professional capacity.
   i. If staff have no option but to use their personal mobile phone for communication with families, they must prefix the dialed number with 141, to hide their own phone number or use Xelion.

Digital cameras

a. Learners under 18 can only be photographed with prior written consent from the parents/carers.
b. Personal cameras are not allowed in the setting and should not be used on off-site activities.
c. PQMS Training has digital cameras and mobile tablets for staff and, where appropriate, for learners, parents/carers, and volunteers to take photographs of learners for display, observations or to support evidence of learning.
d. Use of video equipment can be a legitimate learning/training aid. Learners and parents/ carers should be made aware that this could be part of their learning at PQMS Training.
e. Learners, volunteers, and visitors are not permitted to take photographs or recordings of learners without permission from the CEO
f. No one is permitted to photograph or record images in the toilet area.
g. Learner's images will not be used for promotional or press releases unless prior consent has been given.

Use of other digital devices and programmes.

The principles of this policy apply no matter which current or future technology is used, including computers, laptops, tablets, web-enabled games consoles and smart TV's and whether an app, programme or website is used. If any digital devices are used as part of activities with the business, we would expect all users to adhere to this policy and the guidelines surrounding online use and acceptable behaviour.

D. A. Hudson

Signed:

Dave Hudson
[CEO]