e-Safety and Social Media Policy

Portland Training is committed to the availability of digital technology in order to enhance the learning experience. However, with these new technologies (particularly internet based) comes risks associated with invasion of privacy, cybercrime and safeguarding/prevent issues due to:

- Lack of awareness and understanding of the risks associated with technology and the preventative measures required to prevent hacking, viruses, etc.
- Availability and evaluation of quality information found on the internet in terms of accuracy and relevance.
- Implications of sharing personal information through electronic communication platforms such as email and social media, resulting in inappropriate contact or communication with unknown individuals.
- Copyright infringement due to plagiarism or illegal downloading and sharing of files.
- The taking and distribution of personal images or video footage without an individual’s knowledge or consent.
- Access to illegal, harmful or inappropriate content such as images, video, written media and games.

It is imperative that a dynamic approach is used in order to adapt to the rapidly changing digital landscape, and that a balance is struck between guaranteeing learner safety whilst still ensuring availability of quality digital provision. This is the focus of the e-Safety and Social Media Policy which runs parallel with other relevant policies including the ‘Acceptable Use of ICT’ and the ‘Safeguarding and Prevent Policy’. We believe that safety is as important in the virtual world as it is in the real world.

Scope of Policy

The e-Safety and Social Media Policy applies to staff, learners and any other person or organisation which may have, or require, access to our IT based systems.

Definitions

Internet usage may include (but is not limited to) the following activities:

- Use in the classrooms to support and enrich learning
- Use of social networking, and other web based communication tools that enable learners and tutors to collaborate outside of the training environment to aid learning, research and social exchange.
- Use of online learning and/or undertaking of external assessments/examinations and initial and diagnostic assessments.
- Use of remote learning technologies to complete tutor set work or revision from home or to undertake an online qualification.
- The ability to contact professional organisations and individuals in different fields of expertise for the purpose of technical support and knowledge.
- Enhance staff performance and professional development through access to quality educational materials and good curriculum practice.
- A means of processing and storage of central administration data.
- Remote access to email and electronic documents outside of office hours or when working from home (restricted to staff only)

Responsibilities (Staff)

Internet

You must not access or attempt to access any internet sites that contains any of the following:

- Material of a sexual, pornographic or obscene nature.
- Material of a discriminatory nature.
- Material which promotes an extremist or terrorist ideology.
- Material pertaining to the purchase of firearms.

Should you access any prohibited sites unintentionally, you must report the incident to your Manager or the Contracted Third Party IT Support Provider in order for it to be logged. Deliberate accessing of certain material on Portland Training's ICT equipment or personal devices will be considered as gross misconduct resulting in disciplinary action, which may result in termination of employment. Portland Training have appropriate filters and sonic walls in place to prevent staff or learners accessing any of the content detailed above via laptops or electronic devices and the Contracted Third Party IT Support Provider routinely monitor all equipment to ensure no attempt has been made to access such content. If a website is blocked that staff or learners feel shouldn’t be then a request should be made to the Contracted Third Party IT Support Provider for review.

Social Media

During working hours, staff members should refrain from using social media sites unless they are actively educating learners on the safe usage of platforms like Facebook or Twitter. Staff members may also use Portland Training's official social media accounts with proper authorization.

When social media use occurs, the supervising tutor must ensure compliance with security protocols and privacy settings that safeguard profiles and personal information. Learners may be granted access to WiFi during designated break and lunch times or when internet use is necessary for their program at Portland Training, provided it is available in the learning environment. It is crucial to train learners on responsible social media use during these periods.

Additionally, learners should only use personal electronic devices in the classroom if required for the specific session, as mobile phone usage should be managed by the tutor to maintain a conducive learning environment. Staff members should never intentionally establish social media connections with learners or engage with them through social media or other online platforms.

Direct Messaging using Social Media and Direct Messaging Apps (e.g. WhatsApp)

Portland Training are aware that increasingly learners are most responsive using direct messaging platforms and Social Media messaging services. To that end, Portland Training will allow staff members to communicate with learners and potential learners using these methods when it has been approved by the Line Manager and Designated Safeguarding Lead.

Portland Training recognises the inherent risks associated with the use of these apps and services and therefore all use of said will be reviewed by appropriate Line Managers in consultation with the Safeguarding Team on a regular basis.

E-Safety

Staff members have a crucial role in educating learners, particularly vulnerable groups, about maintaining safety. While regulations and technical solutions like filtering systems hold significance, they should be complemented by a focus on educating learners to adopt responsible practices. The instruction of e-safety to learners is vital when incorporating technology in classrooms. Staff members should serve as positive role models by demonstrating responsible use of ICT (Information and Communication Technology). By striking a balance between regulations, technical measures, and educational efforts, staff can effectively promote a safe and responsible approach to technology use among learners.

Where Internet use is pre-planned in sessions or enrichment activities, learners should be directed to sites which are appropriate for their use and procedures should be followed for reporting any unsuitable material that is found on Internet searches. Where practicable staff should pre-check sites and any possible searches.

Where learners are able to freely search the Internet staff should be vigilant in monitoring the content of websites in case there is any unsuitable material.

Staff should be aware of the potential for cyber-bullying in their sessions where malicious messages e.g. through social networking sites, or text messages on mobile phones etc, which can cause hurt or distress.

It is important to teach learners to develop critical awareness regarding the materials and content they encounter online, guiding them to validate the accuracy of information. Additionally, learners should receive instruction on online safety, emphasizing the significance of creating strong passwords and never sharing personal information on the internet. By equipping learners with these skills and knowledge, they can navigate online platforms with caution, make informed judgments about the credibility of information, and safeguard their personal data in a digital environment.

Portland Training are committed to ensuring all learners are safe and this policy should be read in conjunction with the Acceptable Use of ICT Policy and Safeguarding and Prevent Policy.

Images and Videos

Staff members are strictly prohibited from uploading photos or videos to social media, websites, blogs, or any other online platform without obtaining explicit consent from the learner. In the case of learners under the age of 18, consent must be obtained from their parent or guardian. Any use of photos for marketing or social media purposes should be exclusively handled by the Marketing Team, ensuring that submissions undergo quality and privacy checks through this designated channel. These measures aim to safeguard learner privacy and ensure that all digital content is shared responsibly and with proper authorization.

Email

When communicating with external organisations or learners via e-mail, your allocated work email address should be used at all times. Never make contact with an external organisation or learner from a private email address. Be conscious of the written word and if it could be misconstrued by the recipient, leading to spurious allegations against you.

Although the Portland Training network is protected by anti-virus software, it is still possible for an email containing a virus to arrive in a member of staff's inbox. Attachments should only be opened if they are from a known and trusted source. Files ending in .exe must never be opened.

Passwords to your email account must be kept confidential, be periodically changed (as automatically instructed), and must never be disclosed to another member of staff or learner.

General use of ICT resources

Staff must never adjust any of the settings on their PC/laptop or install any software without the consent of the Contracted Third Party IT Support Provider and Management as it may result in network security being affected. The GDPR Policy should be referenced prior to use of any external devices or media such as USB memory sticks.

General Data Protection Regulation

The protocols detailed in the GDPR and Communications Policy must be adhered to at all times with regard to electronic data, its storage and transmission. Where required, consideration should be given to secure data encryption (contact the IT Desk for assistance),

As per the Acceptable Use of ICT Policy, staff should note that internet and email activity is subject to monitoring.

Related Policies

Acceptable Use ICT Policy

Data Protection and Information Security Policy

Safeguarding Policy

Preventing Extremism and Radicalisation Safeguarding Policy

Staff Code of Conduct

Classroom Management Policy