Oxford Professional Education Group

January 2020

Reviewed Date January 2024

Review Date Jan 2025

Reference number 31

E-Safety Policy

1. Policy Summary

This policy should be read in conjunction with the OXPEG Acceptable Use of ICT Policy.

This e-safety policy applies to all members of OXPEG, including all staff, learners/apprentices, visitors and contractors who have access to, or are users of OXPEG ICT systems and resources, both in and out of learning venues and the working environment, e.g. internet, electronic communications, Virtual Learning Environment (VLE) or mobile devices.

This e-safety policy outlines the learner/apprentice and safeguarding context for the use of the internet and social media and specifies the roles and responsibilities of all those who have access to OXPEG ICT, with specific reference to learners/Apprentices and Designated Safeguarding Leads.

2. What is E-Safety?

The term E-safety is defined for the purposes of this document as the process of limiting the risks to staff, learners/apprentices and authorised contractors when using the internet, digital and mobile technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training.

3. Benefits and Risks

Effective use of social media can bring significant and measurable benefits to OXPEG. These include opportunities to promote OXPEG's success stories, develop national and potentially international reach, improve learner/apprentice engagement and attract high quality staff, learners/apprentices and new business. Social media channels can spread OXPEG's messages quickly and to a large range of audiences at little or no cost and, unlike other traditional media channels, they provide instant feedback from those audiences.

OXPEG provides internet access to some staff, learners/apprentices and authorised contractors, and encourage the use of technologies to enhance skills, promote achievement, enable lifelong learning and develop the business.

Along with these benefits come the risks inherent in managing something that is as dynamic and unlimited in scale. These include the risk of reputational damage arising from misuse by staff, learners/apprentices or third parties, threats to the security of sensitive or confidential information, exposure to malware and a negative impact on productivity.

E-Safety risks can be summarised under the following three headings:

Content

- Exposure to inaccurate or misleading information;
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance, sites promoting radicalisation or pornography;
- Exposure to illegal material, such as images of child abuse;
- Illegal downloading of copyrighted materials e.g. music and films.

Contact

- Grooming using communication technologies, potentially leading to sexual assault, sexual exploitation and radicalisation;
- The use of assumed identities on gaming platforms;
- Bullying via websites, mobile phones or other forms of communication device;
- Spyware e.g. use of Remote Access Trojans/Tools to access private information or spy on their victim.

Commerce

- Exposure to online gambling services;
- Commercial and financial scams.

The requirement to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work for at OXPEG are bound. This e-safety policy should help to ensure safe and appropriate use.

4. Learner/Apprentice Context

To prepare learners/apprentices 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, 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 our staff and learners/apprentices into contact with a wide variety of influences some of which may be unsuitable. These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the learning environment.

Current and emerging technologies in the learning environment and more importantly, in many cases used outside the learning environment by learners/Apprentices include:

- Internet websites;
- Virtual Learning Environments (VLE), Oxcomlearning.com;
- 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.

All of these have potential to help raise standards of teaching and learning but may equally present challenges to both learners/apprentices and trainers in terms of keeping themselves safe. These challenges include:

- Exposure to inappropriate material;
- Cyber-bullying via websites, social media, mobile phones or other technologies;
- Identity theft or invasion of privacy;
- Downloading copyrighted materials;
- Exposure to inappropriate advertising, online gambling and financial scams;
- Safeguarding issues such as grooming (Children or vulnerable adults).

5. Roles and Responsibilities

The key responsibilities of the Designated Safeguarding Lead Paul Jones are:

- Acting as a named point of contact for all online safeguarding issues and liaising with other members of staff and other agencies as appropriate;
- Keeping up to date with current research, legislation and trends regarding online safety;
- Coordinating participation in local and national events to promote positive online behaviour;
- Working with the Information Security Team to ensure that practice is in line with current legislation;
- Maintaining a record of online safety concerns/incidents and actions taken as part of the safeguarding recording structures and mechanisms;
- Reporting to OXPEG Directors and other agencies as appropriate, on online safety concerns and local data/figures;
- Liaising with the local authority and other local and national bodies, as appropriate;
- Working with senior management to review and update the online

safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input;
- Ensuring that online safety is integrated with other appropriate company policies and procedures;
- Meet regularly with SMT who have lead responsibility for online safety.

The key responsibilities for all members of staff and authorised contractors are:

- Contributing to the development of online safety policies;
- Reading the Acceptable Use of ICT Policy and the E-Safety Policy and adhering to them;
- Taking responsibility for the security of company information systems and data;
- Having an awareness of a range of different online safety issues and how they may relate to the learners/apprentices in their care and their colleagues;
- Modelling good practice when using new and emerging technologies;
- Embedding online safety education in learner/apprentice delivery wherever possible;
- Identifying individuals of concern and taking appropriate action by following safeguarding policies and procedures;
- Knowing when and how to escalate online safety issues, internally and externally;
- Being able to signpost to appropriate support available for online safety issues, internally and externally;
- Maintaining a professional level of conduct in their personal use of technology, both on and off site;
- Demonstrating an emphasis on positive learning opportunities;
- Taking personal responsibility for professional development in this area.

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are

still maximised;

- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team;
- To ensure that suitable access controls are implemented to protect personal and sensitive information held on company-owned devices.
- Ensuring that the use of the network is regularly monitored and reporting any deliberate or accidental misuse to the Information Security Manager (ISM)Tricia Wiley

- Report any breaches or concerns to the Information Security Team and ensure that they are recorded, and appropriate action is taken as advised;
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure;
- Report any breaches and liaise with the Information Security Team as appropriate on technical infrastructure issues;
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures;
- Ensuring that the ICT infrastructure/system is secure and not open to misuse or malicious attack;
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all machines and portable devices;
- Ensure that appropriately strong passwords are applied and enforced for all users of company ICT equipment.

The key responsibilities of Learners/Apprentices:

- Contributing to the development of online safety policies;
- Respecting the feelings and rights of others both on and offline;
- Seeking help from their tutor if things go wrong and supporting others that may be experiencing online safety issues;
- Taking responsibility for keeping themselves and others safe online;
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;
- Assessing the personal risks of using any technology and behaving

safely and responsibly to limit those risks.

6. Breach of Legislation or Policy

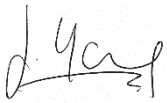
Any suspected breach of this policy may result in disciplinary action and must be reported as an Information Security Incident using the appropriate ISI Recording Form sent to the Information Security Team who will conduct/arrange appropriate enquiries.

Serious offences may lead to dismissal and possibly prosecution.

7. Additional Guidance

In support of this policy, the following online sites provide further information in relation to E-safety and the use of Social Media and the Internet:

- Staying Safe Online – People First: https://www.peoplefirstinfo.org.uk/staying-safe/staying-safe-on-line.aspx
- Get Safe Online: 'The Rough Guide to Online Safety': http://www.getsafeonline.org/media/GetSafeOnline_RoughGuide.pdf
- Thinkuknow: https://www.thinkuknow.co.uk/
- Online Safety – NSPCC: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- BullyingUK: http://www.bullying.co.uk/cyberbullying/how-to-stay-safe-online/

Managing Director:	Jane Young
Signature:	
Date:	January 2022