Oxford Professional Education Group

Reviewed: December 23

Review date December 2024

Reference number 19

ICT Acceptable Use Policy

1. Policy Statement

The Internet is the greatest informational resource, but it can also be an unregulated environment which contains materials that may be illegal in the UK, or unsuitable for employees, learner/apprentices and visitors.

OXPEG is committed to bringing the maximum benefits of ICT to its learners/apprentices and to equipping them with the knowledge, skills and behaviours that will enable them to thrive in the digital age.

ICT exists within OXPEG for the purpose of supporting our role in providing vocational training and assessment. ICT assists OXPEG in discharging these functions and provides learners/apprentices with an opportunity to become familiar with ICT. However, OXPEG recognises that misuse of ICT by learners/Apprentices can occur. This can be by, for example:

- accessing or transmitting offensive or unacceptable material;
- accessing or transmitting extremist or radicalising content.

2. Purpose

The purpose of the policy is to state what is deemed to be acceptable use of OXPEG's computing and ICT resources and support the duty on OXPEG to prevent people from being drawn into terrorism and/or extremism.

3. Scope

All users of OXPEG's ICT facilities and in relation to IT facilities owned, leased, hired or otherwise provided by OXPEG, as well as those connected directly or remotely to OXPEG's network or IT facilities.

It also covers any personal equipment used on our premises, or individuals connecting their own equipment to our network i.e. personal laptops connecting

wirelessly to the internet. ICT facilities include all networks, computer systems and/or computing hardware and software made available by OXPEG.

4. Roles and Responsibilities

Employee and learners/apprentices are responsible for their own actions and are thus liable for any consequences thereof. OXPEG cannot accept responsibility for ensuring that actions of users are acceptable. Whilst we will take steps to monitor use of facilities, we cannot police them absolutely. In all cases the user, or users, concerned will be considered liable for their actions.

Access to and use of OXPEG's computing and IT facilities must comply with UK and International laws.

5. Policy Implementation – Procedures

Auditing and Privacy

In the case of Investigations OXPEG reserves the right to:

- Conduct checks on internet usage, user files stored on the shared drive, OXPEG owned or leased computers, and their usage, where such action is justified for the purposes of system administration, investigation of suspected breaches of the Acceptable Use Policy, to comply with Prevent Duty, or any other lawful purposes;
- Compress, archive, or delete files stored on computing and IT resources, such as shared drive, OXPEG cloud storage or the hard drives of OXPEG owned or leased computers, by existing or past users;
- Access, and, where necessary, to examine the content of user files held on any OXPEG computing and IT resource, private computer connected to OXPEG network, or otherwise downloaded onto personal computers, discs or separate drives for the purposes of investigating suspected breaches of the Acceptable Use Policy, or other lawful purposes;
- Monitor use of OXPEG Wi-Fi by any device including but not limited to computers, laptops, smart phones, tablets, notebooks , log and retain records of all electronic communications (web browsing activities, email exchange etc.) between users of OXPEG ICT and computing facilities, monitor any and all aspects of its telephone and computer system that are made available to staff, students and visitors, and to monitor, intercept and/or record any communications including telephone, e-mail or Internet

communications for the purposes of investigating suspected breaches of the Acceptable Use Policy, or other lawful purposes including Prevent;

To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice Interception of Communications Regulations 2000), employees, Learner/Apprentices and visitors are hereby required to expressly consent to OXPEG doing so.

Breaches of Policy

The list below provides examples of potential ways in which a user may contravene this policy. This list is not exclusive or exhaustive and there may be other matters of a similar nature which would be considered as a breach of this policy. The consequences of the breach will depend on the level of severity:

- Playing computer games;
- Sending nuisance (non-offensive) email;
- Unauthorised access using another user's credentials (username and password) or using a computer in an unauthorised area;
- Assisting or encouraging unauthorised access;
- Sending abusive, harassing, offensive or intimidating email;
- Maligning, defaming, slandering or libelling another person;
- Misuse of software or software licence infringement or Copyright infringement;
- Interference with workstation or computer configuration;
- Theft, vandalism or wilful damage of/to IT facilities, services and resources;
- Forging email; i.e. masquerading as another person;
- Loading, viewing, storing or distributing pornographic or offensive material;
- Unauthorised copying, storage or distribution of software;
- Any action, whilst using OXPEG computing services and facilities likely to bring OXPEG into disrepute;
- Attempting unauthorised access to a remote system;
- Attempting to jeopardise, damage or destroy IT systems security at OXPEG;
- Attempting to modify, damage or destroy another authorised user's data;

- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities;
- Attempting to use OXPEG's ICT facilities, systems and resources to draw people into acts of terrorism or extremism or promoting terrorism/extremism.

Security

OXPEG will endeavour to take reasonable care to ensure that users' data is safe and secure, however this is done in good faith, and no responsibility can be taken for any loss or damage howsoever caused. Facilities are provided "as-is" without any warranty or guarantee of suitability for any purpose, implied or otherwise.

Enforcement

In the event of a known or suspected breach of policy, OXPEG may take immediate action to ensure both the security and accessibility of its computing and ICT resources. Breaches of the Acceptable Use Policy will be dealt with according to their severity.

Incidents which are deemed to be in contravention of this policy will be assessed for their severity and as a result may lead to formal disciplinary action. In extreme circumstances the police may be called. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

Learner/Apprentices and Employees:

Action may consist of (but is not limited to) warnings; suspension or removal of user access to computing and ICT resources, including (but not limited to) services such as e-mail and/or Internet access; and suspension or termination of the user's account. Immediate action does not constitute any judgement of guilt, and appeals may be made.

Employees that identify a suspected breach of the Acceptable Use Policy is responsible for reporting the incident immediately to the Systems Director, Tricia Wiley and preserving any evidence.

For employees, upon receipt of a reported suspected breach of policy an investigation will be carried out and the findings will be considered in accordance with OXPEG's Disciplinary Policy and Procedures.

Appeals
All users are entitled to the right of appeal and any user wishing to appeal must write to the Director Tricia Wiley stating the basis for their appeal.

Usage of Laptops, computers, smart phones, tablets and other devices
Employees, learners/apprentices and others in receipt of an OXPEG owned device should be aware that the device, software and operating system remain the property of OXPEG and are provided on a loan basis only. Additional software MUST NOT be installed, nor hardware modifications made, without authorisation.

Personal use of the ICT system is authorised within reasonable limits if it does not interfere with or conflict with business use. Employees, learners/apprentices and others are responsible for exercising good judgement regarding personal use.

Social Networking
Access to social networking sites has the potential to use significant IT resources at key times of the day and deny access to other users. OXPEG reserves the right to limit access to these sites (e.g. Facebook) from OXPEG owned device.

Computing and ICT Facilities
When using OXPEG computing and ICT facilities users must not:

- Alter any settings;
- Allow other people to use your account,
- Give their password to someone else to use, and/or disclose their password to someone else, and/or be otherwise careless with their password (N.B. personal passwords should be changed regularly);
- Disrupt the work of other people;
- Corrupt or destroy other peoples' data;
- Violate the privacy of other people;
- Offend, harass or bully other people;
- Break the law;

- Waste employee effort or resources;
- Store files not related to their study or work at OXPEG;
- Engage in software piracy (including infringement of software licences or copyright provisions);
- Generate messages which appear to originate with someone else, or otherwise attempting to impersonate someone else;
- Physically damage or otherwise interfere with computing facilities, including attaching any un-approved hardware;
- Waste computing resources by playing games or using software, which is not needed for studies or work;
- Engage in any activity which is rude, offensive or illegal;
- Use the ICT facilities to draw people into terrorism and/or extremism;
- Download and/or run programmes or other executable software from the Internet or knowingly introduce viruses or other harmful programmes or files;
- Enable unauthorised third-party access to the system;
- Use the ICT facilities for commercial gain without the explicit permission of the Director, Tricia Wiley.
- Engage in any activity that denies service to other people or brings OXPEG to disrepute.

When using computing and ICT facilities users may:

- Join a public forum (e.g. social networking site, news group, etc.) if this is a specific requirement of their course or work;
- Only attach headphones and external memory drives to computers;
- Alter computer settings to improve accessibility with the support of an appropriate employee and return to the original settings after use;
- Log out of your account if you are leaving a computer for an extended period of time, or otherwise lock the screen if you leave the keyboard and computer;

- Take appropriate actions to physically secure equipment issued to you for the purposes of study or work.

OXPEG Phones
OXPEG acknowledges that from time-to-time employees or learner/Apprentices may need to make personal calls, this is permissible with permission from a Director or Manager.

Employees with OXPEG provided mobile telephones must remember the phone is for OXPEG's business use only and keep personal calls to a minimum. Employees will be obliged to reimburse OXPEG for excessive private calls made on a phone, when requested to do so.

OXPEG does not allow any members of staff to use mobile telephones when driving on OXPEG business without a hands-free kit. An employee who fails to comply with these procedures may be subject to the Disciplinary Procedure.

Employee Laptops
When issued with an OXPEG laptop, employees will be required to agree to insurance conditions which will include:

- The laptop will at no time be left in a visible position in any unattended, unlocked vehicle but will be placed in the locked boot of a vehicle;
- The laptop will only be kept at OXPEG premises, a private residence or a locked hotel bedroom when away on OXPEG business but will not be taken on a private holiday without OXPEG permission.
- Any room in which the laptop is kept will be secured when unoccupied;
- Agreement to make the laptop available for inspection by directors or managers at any time;
- Agreement to inform OXPEG immediately if the laptop is lost, stolen or damaged;
- Agreement to return the laptop to the employee's line manager on their last day of service with OXPEG;
- Accept responsibility for any damages caused by neglect, misuse etc. excluding reasonable wear and tear;

- Accept responsibility for the cost of repair/replacement of the laptop in the event of a breach of the above conditions.

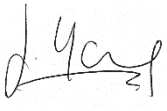
Legal Conformity

Some of the UK legislation applicable to computer use is listed below. Users are reminded of their responsibility to be aware of their legal obligations.

- Obscene Publications Act 1959
- Sex Discrimination Act 1995
- Race Relations Act 1976
- Protection of Children Act 1978
- Data Protection Act 1984
- Telecommunications Act 1984
- Interception of Communications Act 1985
- Copyright, Designs, Patents Act 1988
- Computer Misuse Act 1990
- Criminal Justice and Public Order Act 1994
- Defamation Act 1996
- Disability Discrimination Act 1998
- Data Protection Act 1998
- Human Rights Act 1999
- Regulation of Investigatory Powers Act 2000
- Malicious Communications Act 1988
- Counterterrorism and Security Act 2015

Partners, Accreditations and Awarding Bodies

European Union
European
Social Fund

Signed: 

Date: January 2020