OXFORD
INTERNATIONAL COLLEGE

INTERNET, EMAIL AND TELEPHONE POLICY

POLICY INTENDED FOR:	Staff
CATEGORY:	IT Policies
PUBLISHED:	Server, Policy Folders at College and Students Accommodations, Staff Handbook
POLICY IMPLEMENTED BY:	Principal
POLICY MONITORED BY:	Principal and Operations Manager
REVIEWED BY:	Principal
REVIEWED DATE:	August 2021
CONSULTATION WITH:	Senior Leadership Team (SLT)
RECORD OF CHANGES & ADDITIONS:	Dec 17: Changed he/she to they Jan 20: Amended year of Disability Discrimination Act 2005 and SENDA 2001
NEXT REVIEW:	August 2022

Contents

Introduction

This policy refers to internet usage by employees.

The college acknowledges that employees and tutors need to use the internet and email for legitimate college business and encourages proper usage.

The college requires employees, tutors, and associates to use the internet and emailing efficiently and responsibly.

Any serious misuse of the systems may be regarded as a disciplinary offence.

This policy complies with the applicable laws including (but not limited to):

- Telecommunications Act 1984;
- Copyright, Designs & Patents Act 1988;
- Computer Misuse Act 1990;
- Disability Discrimination Acts 2005 & SENDA 2001;
- Data Protection Act 2018;
- Human Rights Act 1998;
- Regulation of Investigator Powers Act 2000;
- Freedom of Information Act 2000;
- Electronic Communications Act 2000;
- GDPR – May 2018

No provision contained in the policy is intended to contradict or contravene such legislation. Neither is this policy meant to restrict legitimate and authorized college activity.

All college employees and tutors must comply with this policy as set out below and must be aware that the use of any system is not confidential.

The use of the internet and email may be monitored to ensure compliance with college policies and legal requirements.

General Policy Statement

A breach of this policy may result in disciplinary action, in accordance with the college's disciplinary procedure.

In certain circumstances (*e.g.,* using email to communicate obscene material), a breach of this policy may be considered gross misconduct resulting in dismissal.

Use of the College's Systems

The college's systems must not be used inappropriately. The following examples are illustrative but not exhaustive.

School telephones, email, and the internet, including social networking sites, must **not** be used for:

- Harassment or bullying – all communications should be consistent with the equal opportunities and employment laws.
- Private commercial purposes.
- Breaching copyright or confidentiality.
- Intentional propagation of viruses or malware.
- Disrupting or damaging other systems by carrying out acts of a malicious or disruptive nature.

Monitoring Use

The *Regulation of Investigatory Powers Act* does not allow the interception of communications by an employer unless the employer has "lawful authority".

The *Lawful Business Practice Regulations* authorise monitoring for a number of purposes (listed below) and the school will select the least intrusive methods of monitoring.

While the college has no wish to interfere with the privacy of its staff and tutors, it is required to discharge a number of legal duties that are laid down on all employers and managers of computer systems, concerning what passes through and is stored within their systems, for example:

- To ensure that these are not used for criminal or other improper purposes.
- To prevent the spread of computer viruses or malware.
- To avoid other situations that might corrupt or degrade the operation of the school's computer systems or that of other systems elsewhere.

Thus, the college reserves the right to monitor telephone use, internet use, access email and other material on its computer systems, periodically, for various reasonable and necessary purposes including those below:

- Checking compliance with all regulations and policies.
- Preventing or detecting crime.
- Investigating or detecting unauthorized use.
- Checking for viruses or other threats to the performance of the system.
- Investigating abnormal system behaviour.
- Resolving a user problem.
- Monitoring standards of service or training.
- Maintaining or carrying out college business.
- Monitoring of staff and tutors will be kept to a reasonable minimum.

Emails will not be read by anyone, except the sender or recipient, provided they are clearly marked as such. However, this will not be the case where access to the content of the email is required for the prevention or detection of a suspected crime or to prevent the inappropriate use of email.

Any investigation, other than day-to-day monitoring, requires the written authority of the Senior Leadership Team for it to take place. There should be satisfactory, reasonable grounds for the request.

Personal Use

The personal use of email or the Internet, by staff and tutors, is permitted providing that it is not excessive and does not interfere with the proper performance of that person's duties.

It is good practice to maintain a distinction between what is a college business email and what is a personal email, for example by marking personal emails as 'personal'.

Telephones, email, and the internet must not be used to carry out private commercial activities.

Personal telephone calls should be kept as brief as possible. Personal calls should not be made to non-geographic numbers (starting 084 or 087), mobile phones or overseas numbers without prior permission from the Senior Leadership Team (or nominee).

Internet Use

Staff should note that personal use is a privilege and must not be excessive or interfere with the proper performance of an employee's duties.

The internet must not be used inappropriately. The following is an illustrative list of inappropriate use, but it is not intended to be exhaustive. The internet must not be used for:

- Accessing, downloading, storing, recording, or bookmarking sites that are offensive, obscene, defamatory, abusive or otherwise unlawful (for instance, those that facilitate hacking or contain pornographic material)
- Publishing material that brings the school's reputation into disrepute
- Downloading software which breaches the software owner's rights or licence agreements.

Owing to the largely uncontrolled nature of the internet, users can inadvertently access sites containing offensive, obscene, defamatory, abusive, or otherwise unlawful material. In these instances, users must exit such sites immediately. Prolonged or regular access to such sites is considered as intentional misuse of the facility and could lead to disciplinary action.

The school takes no responsibility for any online transactions, not authorised by the Senior Leadership Team, and is not liable for the failure of security measures for use that is not authorised.

The college makes use of internet filtering to safeguard students and staff. Staff must not circumvent the filtering unless authorised by the Senior Leadership Team.

All users should be aware that internet use may be recorded by the college.

Email Use

Email communications are no different, in law, to any other form of written communication:

- They can be legally binding. Consequently, they are actionable within the laws of defamation and libel.
- They are recognised as being capable of contributing to harassment.
- They can create or break contracts.

Emails frequently carry information about individuals' (personal data), in the form of facts, intentions or opinions about individuals.

Therefore, any emails produced in the course of college business, that contain personal data, must be managed in compliance with data protection legislation. This includes the right of individuals to request a copy of the data held about themselves on request.

The email system is the property of the college, but this does not alter the intellectual property rights in the workplace. Staff should note that personal use is a privilege and must not be excessive or interfere with the proper performance of an employee's/tutor's duties.

The email system must not be used inappropriately. The following is an illustrative list of inappropriate use, but it is not intended to be exhaustive.

Email must **not** be used for sending messages that are:

- Offensive
- Obscene
- Defamatory
- Abusive
- Otherwise unlawful.

Emails, like any other form of written communication, can be used as evidence in a court of law.

Access to Email Accounts on Departure

Entitlement to access an individual's email account will automatically cease on the date on which an individual's employment and/or relationship with the college has terminated.

Employees/tutors who leave the school must not access the school's email system for any purposes unless they have the permission of the Senior Leadership Team.

The Senior Leadership Team has the right to curtail access to the internet and/or telephone systems at any time and to report this action to the Proprietor.

Use of Mobile Phones in Vehicles

The Senior Leadership Team takes the view that the use of mobile telephones when driving, even when using a 'hands-free' kit, is dangerous, taking concentration away from the job in hand, i.e. controlling the vehicle. The college's policy is that no member of staff should use a mobile telephone whilst driving on college business. Any person prosecuted for such an act may be subject to disciplinary action.

Mobile phones should only be used in vehicles whilst the vehicle is stationary and parked with the engine off. This includes the use of a 'hands free' kit.

Calls should neither be made nor answered, when the vehicle is in motion, unless someone else is driving.

Use of Mobile Phones on Site

Staff are expected to respect the quiet and privacy of areas such as: common room areas, library, teaching areas. Students may not use mobile phones whilst in lessons.

Responsibilities

The Senior Leadership Team is responsible for:

Making and reviewing the policy

Nominating members of staff to undertake specific duties

Determining an appropriate job description, including the monitoring of the use of the systems

Dealing with any misuse and abuse of the systems

Security and Safety

Users will accept the responsibility for keeping all pornographic material, gambling material, inappropriate text files, material dangerous to the health and safety of students and staff, or files dangerous to the integrity of the college computers from entering the college via the Internet.

- Users will demonstrate legal responsibility by not transmitting any material in violation of UK or Oxford International College regulations. This includes, but is not limited to, copyrighted materials; threatening, harassing or obscene material; pornographic material; material protected by trade secret, or used to promote extremism
- If a user identifies a security problem on the Internet or an Oxford International College computer, he/she is responsible for notifying an administrator or senior member of staff. Users should not demonstrate the problem to other users.
- All users must take responsibility for keeping down costs and avoiding system disruption. No use of the college's access to the Internet shall serve to disrupt its use by other individuals or by connecting networks. It is beneficial for all users to keep the IT systems running efficiently.

Property

Users must respect others' privacy and intellectual property. Any traffic from this network that traverses another network is also subject to that network's acceptable use policy (AUP).

- Users are responsible for citing sources and giving credit to authors during the research process. All communications and information accessible via the network should be assumed to be private property.
- Users will honour the legal rights of software producers, network providers, copyright, and license agreements.
- Users have a right to be informed about personal information that is being, or has been, collected about them, and to review this information.

Behaviours and Consequences

Consequences for inappropriate behaviour are as follows:

- Any violation of the network responsibilities will result in a cancellation of network privileges and may result in disciplinary action. The senior college staff will deem what is appropriate use and their decision is final. Moreover, the senior college staff may deny access at any time, as required. The staff of Oxford International College may request the college's IT providers to deny, revoke, or suspend specific user privileges. Any user identified as a security risk or having a history of problems with other computer systems, may be denied access to the Internet.
- Tampering with computer security systems and/or applications and/or comments will be considered vandalism, destruction, and defacement of college property and dealt with appropriately.
- Vandalism will result in cancellation of privileges and disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or other networks. This includes, but is not limited to, the uploading or creation of computer viruses/malware.

Oxford International College makes no warranties of any kind, whether expressed or implied, for the services it is providing. Oxford International College will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the college's own negligence or the user's errors or omissions. Use of any information, obtained via the Oxford International College computers, is at your own risk. Oxford International College specifically denies any responsibility for the accuracy or quality of information obtained through its services.

FURTHER INFORMATION

For further information about internet, email, and telephony at OIC please speak with Claire Wellstood.

claire.wellstood@oxcoll.com

Operations Manager

Oxford International College

1 London Place

OX4 1BD