310 King Street Melbourne

CRICOS No. 02427A

Registered School No. 2016

Information, Communication and Technology (ICT) Acceptable Use Policy

Policy

At Ozford College (Ozford), information systems, infrastructure and computer networks are an integral part of the learning environment. Ozford has made a substantial investment to create and protect these systems and infrastructure. In addition, there is need that all users access the ICT systems appropriately. As such, access to these systems cannot be provided unconditionally or without limits. This policy outlines the acceptable use of all ICT resources within Ozford.

The aims of the policy are:

- To protect Ozford resources, networks, printers, equipment and other infrastructure and to safeguard the information contained;
- To provide all users with a safe ICT learning environment where the risk of harm including bullying, harassment or discrimination is not tolerated;
- To reduce unsolicited commercial email ("Spam");
- To protect all users from activities that might expose the College or its staff and students to harm and liability.
- To expressly inform all users that everything that they do while connected to the network can be monitored and viewed by authorized personnel.

All Ozford staff and students are bound by this policy.

See also:
Anti-Bullying and Harassment Policy and Procedures
Student Behaviour Management Policy and Code of Conduct

ICT Use Code of Conduct

1. **Security**

   1.1 Staff and students will be provided with an individual user log in and password together with a copy of this ICT Acceptable Use Policy. They are responsible for the security of their passwords and the use of ICT resources via their accounts. Passwords must remain secure and all are expressly prohibited from disclosing their password to any person and from sharing accounts. ICT Department must be informed immediately if any staff or student believes their password has been disclosed and a new password must be reset.

1.2 All PCs, laptops and workstations should be secured by logging off or locking the workstation when the system is unattended.
1.3 Company Resources provided to or accessed by staff and students may contain proprietary and other confidential information about Ozford, its clients, students, employees and suppliers ("**Confidential Information**"). Such information remains the property of Ozford at all times. Staff and students must not copy, duplicate, disclose, or allow anyone else to copy or duplicate any Confidential Information.

2. Privacy, Copyright and Intellectual Property

While Ozford desires to provide a reasonable level of privacy, staff and students should be aware that the data they create on Ozford ICT system is the property of Ozford. Ozford cannot guarantee the confidentiality of information stored on any computer device belonging to the Company or connected to Company Resources.

2.1 Staff and students are responsible for exercising good judgment regarding the use of Ozford ICT resources. The use of Ozford ICT resources is for work related to Ozford and its business operations. Personal use is to be kept to a minimum. Should personal use become excessive, then Ozford may restrict that staff or student's access to Ozford ICT resources or take such other action as deemed appropriate in the circumstances.

2.2 Authorised individuals within Ozford will monitor the equipment, systems and network traffic at any time. Ozford reserves the right to access and audit networks and systems (including electronic mail systems and information stored in the network) on a periodic basis including but not limited to:

- security, network and maintenance purposes;
- assessing the level of personal use;
- accessing or retrieving email or data that may have been deleted;
- ensuring that there is no illegal or improper use of email or the internet;
- monitoring potential breaches of confidential information;
- assessing any violations that may constitute bullying, harassment or discrimination;
- investigating complaints;
- obtaining all data about the use of email and the internet; and
- assessing whether this policy is being adhered to and identifying any possible breaches.

2.3 All users are expected to abide by copyright and intellectual property regulations. If necessary, permission must be sought before uploading or posting images, text, audio and video.

3. External ICT Equipment

Any equipment that is connected to Ozford networks must first be approved by IT Services Division. Approval will be withheld unless there is an active anti-virus program running on the equipment within current anti-virus definitions. Anti-virus software is available from the IT Services Division.

4. Electronic Mail Guidelines

All students and staff are provided with individual email account.

4.1 The contents and size of Employee email accounts must be appropriately maintained by Employees to occupy no more than size limit notified by the Company's IT Services Division from time to time. The Company's servers may enforce size restrictions automatically and notify Employees when the limit is exceeded.

4.2 Some types of emails and attachments are blocked by the ICT systems to help secure the environment from spam, viruses, worms or other harmful software.

5. Internet and Social Media Use

Internet safety is an important issue. Ozford internet service is a filtered service to ensure quality and safety of all users. All users of Ozford internet services are expected to use it in a safe, responsible and ethical manner at all times. This includes:

- Respecting others and communicating with others in a supportive manner, never writing or participating in online bullying (for example, forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours)
- Protecting own privacy; not giving out any personal details, including name, telephone number, address, passwords and images
- Protecting the privacy of others; never posting or forwarding their personal details or images without their consent
- Reporting to a teacher/manager if user feel uncomfortable or unsafe online, or when others participating in unsafe, inappropriate or hurtful online behaviours
- Carefully considering the content before uploading or posting online;
- Investigating the terms and conditions (e.g. age restrictions, parental consent requirements). If unclear seek further explanation from a teacher/manager
- Not bringing to school or downloading unauthorised programs, including games.

6. Personal Mobile Phone, Hand Devices and Computers

Personal Mobile Phone, Hand Devices and Computers are the personal belongings of staff and students. It is the owner's responsibility to ensure they are kept secured and safe. Staff and students are expected to use them in a safe, responsible and ethical manner at all times. This includes:

- Keeping the device on silent during class times; only making or answering calls or messages outside of lesson times (except for approved learning purposes)

- Respecting others and communicating with others in a supportive manner, never verbally or in writing or participating in bullying (for example, harassing phone calls/text messages, forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours)
- Protecting own privacy; not giving out any personal details, including name, telephone number, address, passwords and images
- Protecting the privacy of others; never posting or forwarding their personal details or images without their consent
- Carefully considering the content before uploading or posting online;
- Investigating the terms and conditions (e.g. age restrictions, parental consent requirements). If unclear seek further explanation from a teacher/manager
- Not bringing to school or downloading unauthorised programs, including games.
- Respecting the privacy of others; only taking photos or recording sound or video when I have formal consent or it is part of an approved lesson
- Obtaining appropriate (written) consent from individuals who appear in images or sound and video recordings before forwarding them to other people or posting/ uploading them to online spaces.

7. Prohibited Activities

Under no circumstances is any staff or student authorised to engage in any activity that is illegal under local, State, Federal or international law while using Ozford's ICT system. In addition, the following activities are expressly prohibited:

- Violations of the rights of any person or entity protected by confidentiality, copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use, or the duplication or transmission of copyrighted or otherwise protected materials. This prohibition also applies to materials that are considered "Confidential";
- Sending spam using College ICT system;
- The use of any peer-to-peer file sharing software or websites, including but not limited to BitTorrent, KaZAA, Grokster or Morpheus;
- The use of any IRC or messenger software or websites, including but not limited to AOL Messenger or other "Messengers", IRC or "chat" clients;
- Engage in procuring or transmitting material that is in violation of bullying, harassment, privacy, discrimination or workplace laws including but not limited material which is offensive, obscene, threatening, pornographic, defamatory, discriminatory, insulting, inappropriate, disruptive, intimidating or in violation of a person's privacy;
- Effecting disruptions to, or interfering with, any other computer or network;
- Using any form of network monitoring which will intercept data
- Circumventing user authentication or security of any host, network or account;

- Providing information about, or lists of, Ozford's staff or students to any third party;
- Activities which discredit Ozford or its staff and students;
- Using electronic mail or the internet for political, religious, private commercial, personal profit making, gambling or personal advertising purposes;
- Unauthorised use, or forging, of email header information;
- Connecting to the Internet, or sending email through, an anonymous proxy server or similar conveyance designed to obfuscate the user's identity;
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type;
- Installing any software that is not approved by the IT Department;
- Unauthorised copying of Ozford information to a personal USB memory stick, hard disk or removable storage player (whether it is a music player or otherwise);
- The 'ripping', copying or storage of music for any purpose;

8. ICT Resources Loss/Damage

All ICT infrastructures are covered by a manufacturer's warranty. The warranty covers manufacturer's defects and normal use of the device. It does not cover negligence, abuse or malicious damage.

8.1 Any problems, vandalism, damage, loss or theft of the ICT resources must be reported immediately to the ICT Service Division.

8.2 In the case of suspected theft, a police report must be made by the users and a copy of the report provided to Ozford.

8.3 In the case of loss or accidental damage, a statement should be signed by a user and provided to Ozford. Staff and students may be required to pay for replacement/repair of loss/ damaged ICT resources.

9. Breach of ICT Use Policy

Staff and students are expected to report any wilful damage, suspected breaches of legislation, regulations and Ozford policies and code of conduct. All such reports will be treated in a confidential and responsible manner. Ozford will protect the interests of such staff or student reporting any breaches or suspected breaches in good faith and in a responsible way.

9.1 Depending on the nature of the inappropriate use or breach of ICT resources, non-compliance with this Policy may constitute:

- a breach of Code of Conduct;
- serious misconduct;
- sexual harassment;
- unlawful discrimination;
- a criminal offence

- a threat to the security of Ozford ICT resources;
- an infringement of the privacy of staff, students and other persons; or
- exposure to legal liability.

9.2 Non-compliance with this Policy will be regarded as a serious matter and appropriate action may be taken.

9.3 The Head of IT is responsible in the first instance for handling potential breaches for Users. Formal disciplinary action for staff and students will occur in accordance with Complaints and Appeals policy and procedures.

9.4 Where there is a reasonable belief that illegal activity may have occurred, Ozford has a statutory obligation to report illegal activities and official misconduct to appropriate authorities.