OZFORD
COLLEGE

INFORMATION, COMMUNICATION AND TECHNOLOGY (ICT) ACCEPTABLE USE POLICY AND PROCEDURE

Approving authority	School Council
Purpose	This policy and procedure has been developed to ensure Ozford College protects and safeguards all information collected, provides a safe learning environment involving ICT use that is free from all forms of harm, including bullying, discrimination and harassment.
Responsible Officer	Principal and Academic Director
Associated documents	Anti-bullying and Anti-harassment Policy and Procedure Anti-Discrimination Policy and Procedure Child Safety Policy and Procedure Child Safe Code of Conduct Policy and Procedure Diversity, Cultural Safety and Equity Policy and Procedure Responding to and reporting allegations of suspected child abuse Policy and Procedure Human Resource Policy and Procedure Student Behaviour Management Policy and Procedure Student Support and Services Policy and Procedure Student Complaints and Appeals Policy and Procedure Record Management Policy and Procedure Student Handbook

1. RATIONALE

Information systems and computer networks are an integral part of the Ozford College (the College) business. The College has made a substantial investment to create and protect these systems. IT facilities and services are provided to users to support the strategic objectives of the College.

This policy is designed to allow legitimate and optimal use of ICT facilities and services and to protect both students and the College.

In particular the aims of the policy are to:

- promote the effective use of ICT by students to enable them to work effectively in successfully
- meeting the requirements of their course;
- ensure that ICT resources, networks, printers, equipment and other infrastructure; are
- protected and available for use by students when required;
- protect and to safeguard the information contained within the College's systems;
- reduce unsolicited commercial email ("Spam");

- protect the College and its students from activities that might expose the College or its students to liability.

2. SCOPE

The policy applies to

- to all students who use of the ICT facilities and services;
- computing, collaboration and communications facilities, examples of which include telephones,
- facsimiles, mobile telephones, computers, tablets, printers, photocopiers, emails, internet access, network applications, web services and similar resources;
- the use of the remote system, accessed via IT facilities and services, is also covered by this policy;
- the use of mobile phone, handheld devices, iPads , computers and data storage devices that are the personal belongings of students when they are being used to access or are connected to the College's ICT facilities and services.

3. POLICY

3.1 Users must take responsibility for using ICT facilities and services in an ethical secure and legal manner; having regard for the objectives of the College and the privacy, rights and sensitivities of other people.

3.2 Passwords must remain secure, and all staff and students are expressly prohibited from disclosing their password to any person and from sharing accounts.

3.3 While the College desires to provide a reasonable level of privacy, staff and students should be aware that the data they create on the ICT system is the property of Ozford College.

3.4 College ICT resources provided to or accessed by staff and students may contain proprietary and other confidential information about the College, its clients, students, employees and suppliers ("Confidential Information"). Such information remains the property of Ozford College at all times. Staff and students must not copy, duplicate, disclose, or allow anyone else to copy or duplicate any Confidential Information.

3.5 The use of College ICT resources is for work related to the College and its business operations. Personal use is to be kept to a minimum. Should personal use become excessive, then the College may restrict that staff or student's access to ICT resources or take such other action as deemed appropriate in the circumstances.

3.6 All users of the College internet services including the intranet and any social media 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 or harassment (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 a concern if the student or staff member feels uncomfortable or unsafe online, or when others are 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
- abiding by copyright and intellectual property regulations. Permission must be sought before uploading or posting images, text, audio and video.
- Not bringing to school or downloading unauthorised programs, including games.

3.7 When participating in internet or social media use in a personal capacity, either at work or at home, where the students or staff member can be associated with the College in any way, the person must not:
- Post anything that is obscene, defamatory, threatening, bullying, discriminatory, hateful, abusive or unlawful.
- Disparage or be disrespectful of the College, or other employees, contractors, volunteers or students of the College.
- Identify or discuss students or staff members or post photographs that include the College's staff members, unless permission is first obtained from the staff member.

3.8 Staff and students are expected to use Personal Mobile Phone, Hand Devices and Computers in a safe, responsible and ethical manner at all times.

3.9 Under no circumstances are any staff or students authorised to engage in any activity that is illegal under local, State, Federal or international law while using the College ICT system.

3.10 The College may monitor users' use of the College resources.

3.11 The College may monitor the equipment, systems and network traffic of users at any time.

3.12 The College can access and audit networks and systems (including electronic mail systems and information stored in the network) on a periodic basis for any business purpose 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 harassment or discrimination;
- investigating complaints of users, clients or suppliers;
- obtaining all data about the use of email and the internet for strategic purposes; and,
- assessing whether this policy is being adhered to and identifying any possible breaches.

3.13 Staff and students may be required to pay for replacement/repair of loss/ damaged ICT resources in the case of negligence, abuse or malicious damage.

Prohibited Activities

3.14 Under no circumstances is a student authorised to engage in any activity that is illegal under local, state, federal or international law while using College resources.

3.15 The following activities are expressly prohibited:

- Violation 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 the College ICT system;
- The use of any peer-to-peer file sharing software or websites, including but not limited to BitTorrent, eMule, LimeWire, Ares, 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, the College’s staff or students to any third party;
- Activities which discredit the College 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 ICT Services Division;

- Unauthorised copying of College information to a personal USB memory stick, hard disk or removable storage player (whether it is a music player or otherwise); and
- The 'ripping', copying or storage of music for any purpose.

Review

3.16 As required by Ministerial Order 1359 Managing the Risk of Child Abuse in Schools and School Boarding Premises, this policy is reviewed after any significant child safety incident, or at least every two years, and improved where applicable.

4. PROCEDURE (ICT Use Code of Conduct)

4.1 The ITS Services team has responsibility for this policy.

Security

4.2 Staff and students will be provided with an individual user log in and password together with a copy of this **ICT Acceptable Use Policy and Procedure**.

4.3 Staff and students are responsible for the security of their passwords and the use of ICT resources via their accounts.

4.4 The ITS Services team must be informed immediately if any staff or student believes their password has been disclosed and a new password must be reset.

4.5 All PCs, laptops and workstations should be secured by logging off or locking the workstation when the system is unattended.

Privacy, Copyright and Intellectual Property

4.6 Staff and students are responsible for exercising good judgment regarding the use of College ICT resources.

4.7 The College 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.

External ICT Equipment

4.8 Any equipment that is connected to College networks must first be approved by the ICT Service Division. Approval will be withheld unless there is an active anti-virus program running on the equipment within current anti-virus definitions.

4.9 Anti-virus software is available from the ITS Services team.

Electronic Mail Guidelines

4.10 All students and staff are provided with individual email account.

4.11 A signature should be present on all email correspondence.

4.12 The contents and size of Employee email accounts must be appropriately maintained by Employees to occupy no more than size limit notified by the ICT Services Division from time to time.

4.13 The servers may enforce size restrictions automatically and notify when the limit is exceeded.

4.14 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.

Internet and Social Media Use

4.15 All staff and students are informed about the internet use requirements as part of their orientation.

4.16 The College's internet service is a filtered service to ensure quality and safety of all users.

Personal Mobile Phone, Hand Devices and Computers

4.17 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.

4.18 Staff and students are expected to use Personal Mobile Phone, Hand Devices and Computers 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 there is 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.

ICT Resources Loss/Damage

4.19 All ICT infrastructures are covered by a manufacturer's warranty.

4.20 The warranty covers manufacturer's defects and normal use of the device. The warranty does not cover negligence, abuse or malicious damage.

4.21 Any problems, vandalism, damage, loss or theft of the ICT resources must be reported immediately to the ITS Services team.

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

4.23 In the case of loss or accidental damage, a statement should be signed by a user and provided to the College.

4.24 Staff and students may be required to pay for replacement/repair of loss/ damaged ICT resources in the case of negligence, abuse or malicious damage.

Breach of ICT Use Policy

4.25 Staff and students are expected to report any wilful damage or breaches of this policy.

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

4.27 The Head of the ITS Services team is responsible in the first instance for handling potential breaches of this policy. The Student Services team will provide support in the case of any student related matter.

4.28 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 College ICT resources;
- an infringement of the privacy of staff, students and other persons; or
- exposure to legal liability.

4.29 Staff will follow one or more of the following policies in resolving the matter:

- **Anti-Bullying and Anti-Harassment Policy and Procedure**
- **Anti-Discrimination Policy and Procedure**
- **Child Safety Policy and Procedure**
- **Diversity, Cultural safety and Equity Policy and Procedure**
- **Responding to and Reporting Allegations of Suspected Child Abuse Policy and Procedure**
- **Human Resources Policy and Procedure**
- **Student Complaints and Appeals Policy and Procedure**
- **Student Behaviour Management Policy and Procedure**

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

5. FEEDBACK

Feedback or comments on this policy and procedure is welcomed by the listed responsible officer.