



## Oakleigh Grammar

<b>Policy Document Name</b>	ICT Acceptable Use Policy
<b>Date Ratified by Management Committee</b>	May 2016
<b>Date for Review</b>	June 2019

### **PREAMBLE**

The School's IT Systems play a pivotal role in realising the School's Strategic Plan objective. Oakleigh Grammar promotes staff and students to use ICT in an appropriate manner in relation their respective needs.

The School embraces student use of ICT in the belief that it enables students to learn in a multitude of different and powerful ways with great efficiency. ICT use is pivotal in ensuring that education embraces the concept of learning anywhere and at any time.

The school is committed to the use of electronic communications in the conduct of school business and affairs, whilst at the same time ensuring that the use of electronic communications:

- Protect personal privacy
- Does not breach applicable laws
- Does not adversely affect the School's commercial interests

The purpose of this policy is to clarify what constitutes acceptable and unacceptable use of Information and Communication Technologies (ICT).

This policy is to be read in conjunction with the student. Acceptable use policy found in Student Planner and Mobile Phone and Electronic Devices policy the Student Welfare policy, Wireless Network Policy as well as the Harassment – Discrimination and Grievance Policy.

### **PURPOSE**

#### **The Role of Students**

Students are responsible for their own behaviour and actions. They are careful and respectful when using School's ICT facilities and devices.

Students understand and respect that there will be times when their parents and teachers wish for them not to make use of ICT. At school, some learning will occur that does not require the use of a device. At home there will be times when parents wish for their children to 'disconnect' from schoolwork or socialising with friends.

Students understand and respect the need for staff and parents to check what they have been doing with the device. These checks will be conducted randomly throughout the whole school year.

Students are cybersmart and take reasonable precautions to avoid online dangers, as outlined on the Cybersmart website ([www.cybersmart.gov.au](http://www.cybersmart.gov.au)). Specifically they are familiar with:

- avoiding unwanted contact;
- sexting;
- cyberbullying;
- preserving digital reputation;
- trusting online friends;
- digital footprints;
- offensive content;
- identity theft.

## **PURPOSE**

### **The Role of Parents/Guardians**

Parents and Guardians are ultimately responsible for setting and conveying the standards that their children should follow. The School expects that those standards will be in accordance with School rules, this Policy and other School Policies.

### **The Role of Teachers**

Teachers will embrace student use of ICT in the belief that it enables students to become more powerful and efficient learners. They will provide guidance and instruction to students regarding appropriate use.

### **Training of staff**

### **The Role of the School**

The School undertakes a commitment to implement and uphold the **ICT Acceptable Use Policy** and to provide appropriate physical and financial resources to enable safe and educationally relevant access to ICT.

### **Personal Devices**

Students are permitted to use their iPad on the school network for educational purposes. However, all content stored on, or accessed from, the device must fit within the values of the School. If a student brings their personal device to school and the device includes any inappropriate material, the school reserves the right to request that it be immediately removed and may take further disciplinary action.

### **Unacceptable Use**

When using ICT, students should be aware of the issues relating to privacy of both themselves and others. Students should take the utmost care when using ICT equipment as it is easily damaged and expensive to replace. Explicitly students should not:

- capture or distribute voice recordings, still images or moving footage of any person without their permission;
- access, create or distribute offensive material;
- post personal details about themselves or others in electronic public spaces;
- share their user name or password with others;
- play games without permission;
- delete their internet history;
- attempt to enter any area of the School network/intranet to which they do not have access rights;
- use proxy internet websites to access web content that has been restricted by the School.

Please note the School prohibits student use of any form of portable wireless device, apart from the School sanctioned iPads, on the School network.

## **Disciplinary Actions**

Generally, classroom teachers and home group teachers will ensure that appropriate consequences are put in place for inappropriate student behaviour. Process for management of students with iPads exists and is to be followed by staff. Serious misuse will be dealt with by the Head of School, Deputy Principal and or the Principal.

Processes for management exist and should be applied. They can be found in the student planner. Students and parents must sign the ICT Acceptable Use policy in the planner.

## **Systems Configuration**

The School will supply all users with IT hardware and software in a standard configuration. Changes to this configuration for personal reasons are prohibited. The support of standard configuration simplifies problem rectification. Should support be required for a non-standard machine, the standard image or configuration will be reloaded prior to support being carried out.

All devices must be registered using their MAC address onto the School network.

## **Systems Care**

All ICT equipment is to be handled with care and respect. Storage in correct cases, keeping the equipment with you as much as possible and storing out of sight are highly recommended. Damage to ICT equipment caused by neglect or improper use could, in extreme cases, be charged to the user directly.

All ICT equipment provided to a user remains the property of the School at all times.

A user to whom a laptop, desktop or other device is lent, is responsible for the care and security of that device at all times, and must not lend it to any other person without the permission of IT Support. It is not envisaged, for example that a teacher would lend a device to another member of his/her family.

ICT equipment in classrooms is provided to assist in student learning, and should not be used outside these purposes. Staff should use their School issued iPads when teaching in a classroom rather than using a student workstation.

Users should be aware that if they do not adhere to this policy and their laptop, desktop or other device is stolen, the School reserves the right to take reasonable steps to recover the costs associated with replacing the equipment.

Users of School devices must sign a device loan agreement to be renewed at the end of each year.

## **Password Security**

The security and protection of individual passwords is a prime responsibility of the individual owner of the password. Therefore, if something is authored from a password protected system, it will be assumed that the owner of the password is also the author. Passwords are not to be stored on your device and need to be of a safe and complex nature, i.e. including words, number and or symbols.

All users must be responsible in ensuring the secrecy of their password. For example:

- A person's username and password must not be shared with any other person
- A password must not be written down and left in a place where it can be easily found
- Precautions must be taken to prevent a password being copied, observed or overheard
- A person must change his/her password if they suspect someone else knows it or if directed by IT Support Staff

## **Property and Copyright Information**

Users of the School's IT Systems should respect the intellectual property rights of others. In particular, users should be conscious of the provisions of the Australian Copyright Act which in general terms (subject to some exceptions) prevents a person from copying, reproducing, and making public, adapting, broadcasting or transmitting copyright material owned by another person without permission. The Copyright Act 1968 makes it clear that these restrictions continue to apply to an online environment. Users should be aware that material may still be subject to copyright even if it does not contain a copyright notice or copyright symbol.

## **Virus Control**

The school uses a centralised network and stand alone virus checking software that is updated regularly. It is the responsibility of all users to ensure that all software sourced externally from the School is virus checked prior to loading on local or network drives. If a user knowingly introduces a virus or fails to follow the above policy, action will be taken.

## **Email and Internet Usage**

The School provides access to email and Internet facilities for school communication, with educational imperatives and supporting the objectives of the School in mind. Inappropriate use of these facilities can have considerable consequences. Inappropriate use may pose a threat to system security, the privacy of our users, customers and employees and maybe also endanger the legal liability of the school.

The School recognises that the Internet and intranet are useful resources for general research purposes and to organise social activities. Incidental and occasional personal use of our communication systems is, therefore, permitted.

Users must exercise great care when composing email messages. Appropriate etiquette should be observed in email messages and the use of impolite or inflammatory language should be avoided.

Some electronic communications may constitute bullying, discrimination or sexual harassment and may be in breach of the School's policies. Your intention in writing or sending a message is irrelevant. If the message offends, humiliates or intimidates another person, it may breach our policy and relevant legislation. The School and/or individuals may be held liable for the content of messages which are offensive, and external tribunals may request copies of documents as discoverable if a complaint of harassment or discrimination is made against you or the School.

Email users must comply with any operational restrictions of the School which may be in place from time-to-time. Users should be aware that if a court subpoenas email records, the School must comply.

Users must be aware that email messages which they send may be construed as representing the School's position. Where a user does not have authority, is not aware of the School's position or where his or her personal view may differ from that of the School, the message should state that the opinion expressed is that of the writer and does not necessarily reflect the views of the School.

All email traffic through the Schools information technology systems is subject to monitoring by IT Support and should not be deemed as private.

## **Social Networking and Blogging**

Interacting on blogging and social networking sites such as Blogger, Tumbler, Twitter, Facebook, MySpace, YouTube, Skype, Instant Messaging Services and other related sites ('Social Networking') by users, whether using the School's IT Systems or personal devices both on and off Campus, are also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the School's IT Systems to engage in Social Networking is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate School policies, is not detrimental to the School's best interests, and does not interfere with a user's regular duties.

Oakleigh Grammar's Confidentiality policy also applies to Social Networking. As such, users are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Oakleigh Grammar's Confidentiality policy when engaged in Social Networking.

Users shall not engage in any Social Networking that may harm or tarnish the image, reputation and/or goodwill of the School and/or any of its users. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when Social Networking or otherwise engaging in any conduct prohibited by the School's Bullying, Non-Discrimination and Anti-Harassment policies.

Users may also not attribute personal statements, opinions or beliefs to the School when engaged in Social Networking. If a user is expressing his or her beliefs and/or opinions while Social Networking, the user may not, expressly or implicitly, represent themselves as a user or representative of the School.

Users assume any and all risk associated with Social Networking. Apart from following all laws pertaining to the handling and disclosure of Copyright Materials, Oakleigh Grammar's trademarks, logos and any other intellectual property may not be used in connection with any Social Networking activity.

### **Document Retention and Backup**

Users must be aware that deleted data (including both files and email) can, in most cases, be recovered and used in disciplinary proceedings, litigation or criminal proceedings.

### **Welfare and Privacy**

The School's IT Systems must not be used to compromise the welfare or interfere with the privacy of others.

Both the School and Users are required to comply with Federal and State legislation which may apply from time-to-time with respect to privacy of personal information.

### **Other Prohibited Uses**

Other prohibited uses of the School's IT Systems include, but are not limited to:

- The unauthorised use of passwords to gain access to another user's information or communications except as set-out in the Access and Disclosure section of this document.
- Using the School's IT Systems for electronic 'snooping'; i.e., to satisfy idle curiosity about the affairs of others, with no business reason for obtaining access to the files or communications of other (this prohibition applies to all users, including IT Support administrators and supervisors)
- Using the School's IT Systems to solicit or conduct business other than the business of the school.

### **Consequences if this Policy is breached**

Any use of the School's IT Systems contrary to this policy may result in a withdrawal of access or other disciplinary action. In the case of students, it may also be dealt with under the Student Welfare Policy.

In the event of what the School considers to be a serious breach by a user, disciplinary action may be taken against those users which may result in counselling, warnings or dismissal/expulsion. Any breach of Federal or State laws could also result in criminal charges being brought to bear.

## **Cyber Bullying, Peer Pressure, Spam**

Students must not engage in bullying, spamming, illegal behaviour, malicious blogging or similar antisocial behaviours. Students who engage in antisocial behaviours in a social networking or blogging site that have ramifications within the School community (such as bullying a fellow student) will be subject to School regulations regarding such behaviour even though the infringements occurred outside the school.

### **Advice to Students**

Students are advised never to offer any personal information including last name, contact information, home address, phone numbers, school's name, e-mail address, last names of friends or relatives, instant messaging names, age, or birth date.

Students are advised never to post provocative pictures of themselves or anyone else, and be sure any images you provide do not reveal any of the previously mentioned information. Remember to also check the background of a picture.

Students are advised to use blogging provider sites with clearly stated terms of use, and make sure they can protect the actual blogs, not just the user accounts, with password protection. However, it is prudent to presume that anyone can see it.

### **Teacher-Student Relations**

Teachers hold a particular and special position in society and are expected to uphold moral and ethical codes of behaviour, often to a greater degree than any other profession or vocation.

Teachers should, as a rule, not have external friendships (i.e. personal relationships) with current students beyond that which is normal for the teacher/student relationship. A personal relationship on a SNS would exceed the accepted bounds of a teacher/student relationship and might leave the teacher open to allegations of improper conduct.

Teachers need also to be aware of interaction with the parents of current students in that comments or opinions may be construed in ways not envisaged that may lead to unforeseen social or legal complications (see Legal Liability below).

Friendships (personal relationships) with ex-students are a matter for the individual teacher but it is prudent to consider the ramifications of personal relationships with ex-students who have younger siblings or friends still at the school, where private or personal information could be passed on to third parties.

### **Use**

The School ICT Network is for educational purposes.

When using it the student must:

- respect the rights of others to access resources for teaching and learning, to privacy and good reputation;
- follow School rules, and State and Federal laws.

Some personal use is allowed, but it must be with permission and must not interfere with school work, disrupt the system or harm the School's reputation.

Not allowed:

- anything which harms the reputation of Oakleigh Grammar School or its staff and students;
- sending confidential Oakleigh Grammar information to persons outside the School without permission;
- sending private information such as e-mail and web addresses without permission;
- activities which would damage the security of the system, such as hacking, use of others' passwords;
- breaking laws of copyright, moral rights or intellectual property – note: this includes illegal copies of software, music, video, images;
- On-line games, gambling, chain mail, SPAM;
- activities which might disrupt the network such as large email distribution lists or large attachments; large downloads or uploads;
- mobile phone use is not allowed in class or assembly time. Phones must be turned off at such times, unless authorised;
- Misuse of hardware which would lead to damage, loss or theft. Defects and damage must be reported to IT Support.

### **Content**

Content of electronic software, documents, files, faxes, web pages, intranet, mobile phone messages and emails:

- must not harm the reputation of the School, staff or students if it was seen by members of the public;
- must be legal.

Material published on School Web pages or Intranet should follow good practice publishing standards and laws.

Not allowed:

1. Inappropriate, offensive or illegal material, such as anything that:

- would cause offense to students, teachers or parents such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism, ageism;
- is derogatory or threatening to another: libellous, slanderous, inflammatory, threatening, harassing;
- has intention to deceive, impersonate or misrepresent;
- is Copyright material – except: small amounts of some material may be copied and communicated for your private study. Refer to OG Copyright compliance documents.

2. Inappropriate material accidentally accessed on Internet or received via email:

- immediately leave site or delete email. Advise IT Support if material is illegal;
- SPAM or Chain mail: delete, do not respond, advise IT Support if it contains offers of illegal material or services.

3. Forwarding emails without permission of sender or which contain copyright material (see above note about Copyright).

### **Virus protection**

All machines connected to the ICT System must have adequate anti-virus protection regularly updated.