OAKLEIGH GRAMMAR	**Oakleigh Grammar**
Policy Document Name	**ICT Acceptable Use Policy, including Social Media**
Date Ratified by Board of Management	July 2025
Date for Review	July 2028

1. 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 to 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 to conduct of school business and affairs, whilst at the same time ensuring that the use of electronic communications:

- Does not increase the risk of child abuse
- Protect personal privacy
- Does not breach applicable laws
- Does not adversely affect the School's commercial interests

This policy is to be read in conjunction with the Student Acceptable Use Policy found in the student diary and Mobile Phone and Electronic Devices Policy, The Student Welfare & Behaviour Management Policy, as well as the Harassment, Discrimination and Grievance Policy, and Child Safety & Wellbeing Policy.

This policy covers students, employees, contractors and volunteers to the School. This policy also applies to all ICT usage on campus, during school-related activities off-site, and during remote or hybrid learning. It also applies to the use of personal devices when connected to the school network (BYOD).

Definitions

- **ICT (Information and Communication Technology)**
  Refers to all digital technologies used to access, create, communicate, and manage information. This includes computers, tablets, mobile phones, the internet, software applications, and school networks.

- **Generative AI**
  Refers to artificial intelligence tools that can produce new content such as text, images, audio, or video in response to prompts. Examples include ChatGPT, DALL·E, and other AI-based writing or image tools.

- ***Personal Devices***
  Refers to privately owned digital devices such as smartphones, tablets, or laptops that students or staff bring to school and use for learning or communication.

- ***Cyberbullying***
  The use of digital technologies to deliberately and repeatedly harm, harass, or intimidate another person. This includes sending hurtful messages, spreading rumours online, or posting embarrassing images.

- ***Social Media***
  Online platforms or applications that allow users to create, share, and interact with content and others. Examples include Instagram, Facebook, WhatsApp, Snapchat, TikTok, and YouTube.

- ***Digital Footprint***
  The record or trail of a person's activities online, including websites visited, social media activity, shared content, and personal information. Digital footprints can be permanent and visible to others.

2. Purpose

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

The Role of Students

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

Students are encouraged to understand and respect that there will be times when their parents and teachers do not wish for them to make use of ICT. At school, 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 are encouraged to 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 encouraged to demonstrate digital citizenship by using technology in ways that reflect the values of respect, responsibility, and integrity. This includes treating others with kindness in online spaces, thinking critically before sharing content, and engaging ethically with digital tools and platforms. Students should take care to protect their privacy, respect the rights of others, and use their digital voice to contribute positively to the school and wider community. By making thoughtful and ethical choices online, students help create a safe, inclusive, and respectful digital environment for everyone.

Students are encouraged to be cybersmart and take reasonable precautions to avoid online dangers, as outlined on the eSafety Commission (www.esafety.gov.au). Specifically they are to be familiar with:

- avoiding unwanted contact;
- sexting;
- cyberbullying;

- preserving digital reputation;
- trusting online friends;
- digital footprints;
- offensive content;
- identity theft.

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 related 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, according to School Policies.

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

Use of Generative AI Tools (e.g. ChatGPT, etc.):
Students may engage with Generative AI tools for educational purposes under teacher guidance. These tools must be used responsibly, ethically, and in accordance with the School's values. Usage must not involve entering sensitive personal data or content that could identify an individual. Primary students may only use AI tools in tightly controlled settings with explicit teacher supervision.

Parents/Guardians acknowledge that such tools may be used in classroom settings, and student interactions with them will be monitored. Students aged under 18 must have parental consent for accounts where required under provider terms. The School reserves the right to restrict or revoke use if misuse is identified. Parental consent is required and documented for students under 18 where platform terms of service require it. Consent is collected at the beginning of the academic year.

3. Personal Devices
Students are permitted to use their iPad, laptop or other personal devices 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 a 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.

4. 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 and devices 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, including those that may be generated by Generative AI Tools;
- Post personal details about themselves or others in electronic public spaces;
- Share their user name or password with others;
- Play games without permission;
- 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.

5. 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, laptops and other personal devices and computers exists and is to be followed by staff. Serious misuse will be dealt with by the Year Level Leaders, Curriculum Leaders, Assistant Principals, 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 at the commencement of the year.

6. 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.

7. Systems Care

All ICT equipment is to be handled with care and respect. Storage in correct cases, keeping the equipment with the individual 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 by the School, 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. A teacher must not, without good cause, lend a device to another member of his/her family for any significant amount of time.

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 or laptops and avoid using student devices at all times

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 associcated with replacing the equipment.

Users of School devices must sign a device loan agreement and/or have their device recorded as being ‘loaned’ from the IT department.

8. Cybersecurity Practices and Password Security

All users are expected to maintain good cybersecurity habits to protect personal data and the School's digital systems. This includes using strong, unique passwords and enabling multifactor authentication (MFA) where required. Users must be cautious of suspicious emails, links, or messages and report any phishing attempts or unusual activity to IT Support immediately. Regular software updates and responsible use of devices are essential in preventing security breaches. By staying alert and following these practices, we help ensure a safe digital environment for all.
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 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 responisble 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

9. 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.

10. 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.

11. 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 is a useful resource 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 not be used.

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 School's information technology systems is subject to monitoring by IT Support and should not be deemed as private.

12. Social Media

a. Overview

Social media is any form of online or web-based publication, forum or presence that allows interactive communication, including, but not limited to, Facebook, Linkedin, Facetime, WeChat, WhatsApp, Instagram, Snapchat, forums, blogs, discussion board chatrooms, Twitter, podcasts, video conferencing, instant messaging and YouTube. These channels offer individuals the opportunity to connect with people, create, upload and share information and ideas, and develop relationships through online communities and networks.

There is great potential for the use of social media in school communities in terms of educational outcomes and as a means of communication. Students and employees need to understand the expectations of the School when using social media in a professional and social capacity.

Limited and occasional use of the School's IT Systems to engage in the use of social media 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.

Users assume any and all risk associated with using social media.

b. Social Media Risks

The following are some of the major risks associated with the use of social media:

- Reputational damage to organisations and people;
- Disclosure of confidential information and breach of privacy laws;
- Posting of offensive, bullying, harassing and discriminating material;
- Misuse of intellectual property and breach of copyright laws; and
- For teachers, breaching the Victorian Teaching Profession Code Of Conduct

c. Guiding Principles

i. Employees

The School recognises that employees may use social media in their personal life; however, such use may have a negative impact on the School. The School expects that employees will always act in the best interests of the School when communicating in an online environment.

It is important for employees to recognise:

- Online behaviour should always demonstrate respect for the dignity of the each person;
- The need to behave in an ethical manner and that any communications are consistent with the values of the School and professional expectations and standards;
- Their ability to serve as role models to students and as a representative of the School
- Social media activities may be visible by current, past or prospective staff, students and parents

Accordingly, employees' personal use of social media must:

- Not bring the school into disrepute or interfere with, or compromise their duties or responsibilities to the School or students
- Comply with other School Policies and Professional Standards in respect to Professional Boundaries, Codes of Conduct, Harassment and Grievances, and Privacy, when posting personal comments that relate to, or can be identified as relating to School issues (e.g. referencing employees, students, policies). Employees must not, under any circumstances, disparage or speak adversely about the School, School business matters or activities, its staff, or its students or parents through social media channels.
- Comply with all laws and policies pertaining to the handling and disclosure of copyright materials and any other intellectual property.

To avoid potentially breaching this policy or compromising the professional expectations of them as employees at the School, employees' use of social media may not involve connections with the following persons on social media (e.g. being "friends" or connections):

- Recent former students (i.e. enrolled at the School within a two-year period before connecting);
- Parents of current students

unless special circumstances exist (e.g. staff member is a parent of a current student, a parent is a personal friend or relative, the teacher is a relative of the student) and the employee has advised the Principal of the connection.

An exception to this could be through professional associations, for example, via LinkedIn.

Friendships (personal relationships) through social media platforms 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.

Employees must not connect with current students or interact with, or post images of, students on their own private social media. Personal relationships with current students via social media channels (for example, adding a current student as a "friend" or "follower" on Facebook, Twitter, Instagram or equivalent) exceed the accepted bounds of a teacher/student relationship, and may leave the employee open to allegations of improper conduct.

An exception to this requirement is when prior approval for the connection has been obtained from the Principal on the basis that an employee and student has a legitimate purpose.

Employees must not post images that include Oakleigh Grammar staff or students on social media channels unless authorised by the School, and not without prior consent of the individual(s) involved.

Work Related
The use of online learning communities by employees for educational purposes or school related activities must be in accordance with the other relevant School policies and procedures relating to online learning.

It is expected that the main form of online communication between staff and students is via the school email system and Learning Management System (e.g. Compass). Any other collaborative learning space, blog, wiki, or forum must be approved by the relevant Assistant Principal – Academic or Deputy Principal before it is established and staff may only use a professional account, not their personal account. Examples where approval may be granted by the A include:

- Closed Facebook pages for VCE Units 3-4 subjects, where there are no links to a staff member's personal social media account.
- Shared WeChat groups for the welfare needs of our international students
- When groups travel on extended school tours and the use of, for example, WhatsApp or WeChat, is being used in case of emergency or a welfare need.

In these situations, connections should cease when the tour concludes, a student leaves the school or no longer enrolled in the specific subject.

All communication between staff and students must reflect a professional relationship.

ii. Students
It is recognised that students may use social media in their personal life. However, it is also recognised that such use may impact on their school – student relationship

It is important for students to recognise:

- Online behaviour should at all times demonstrate respect for others;
- The importance of protecting their privacy;
- The need to behave in an ethical manner and that any communications be consistent with the values of the School and reflect responsible citizenship;
- Social media activities may be visible to others or able to be *screenshotted* for later use;
- Comments and images may be uncontrolled once they are posted. Online material effectively lasts forever and may be replicated endlessly. Online material may also be viewed by recipients who never expected to see it or who may see it out of context. Inappropriate remarks, content and information could also damage the School's reputation or an individual's reputation.

Students are advised to never:

- Post personal details about themselves or others in electronic public spaces 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.
- Post images that may reveal any of the previously mentioned information, including in the background;

- Share their user name or password with others;
- Post provocative pictures of themselves or anyone else.

Students must not:

- Engage in bullying, spamming, illegal behaviour or similar antisocial behaviours;
- Capture or distribute voice recordings, still images or moving footage of any person without their permission;
- Access, create or distribute offensive or illegal material, including those that may be generated by Generative AI Tools;

Students who engage in antisocial, offensive or illegal behaviours in a social media site that have ramifications within the School community (such as bullying a fellow student, or posting negative comments about the School or others) may be subject to School regulations regarding such behaviour even though the infringements occurred outside the school. This may also involve the police.

Students should have the permission of other students when posting images from a school related event on their personal social media sites.

Students should not post images of any staff member without their consent.

13. 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.

14. Welfare and Privacy

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

Reporting ICT Concerns

Students and staff are encouraged to report any misuse of ICT systems, incidents of cyberbullying, or concerns related to online safety as soon as possible. Reports can be made directly to a trusted teacher, Year Level Leader, IT Support or the Deputy Principal. All reports will be treated seriously, investigated appropriately, and handled with discretion to ensure the safety and wellbeing of everyone in the school community.

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.

15. 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.

16. 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, dismissal/expulsion or termination of employment. Any breach of Federal or State laws could also result in criminal charges being brought to bear.

17. Use of the School Network

The School Network is for educational purposes. Whilst 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.

When using it the student or staff member 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.

The following usage is 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;
- Gambling, chain mail, SPAM;
- Activities which might disrupt the network such as large email distribution lists or large attachments; large downloads or uploads;
- Misuse of hardware which would lead to damage, loss or theft. Defects and damage must be reported to IT Support.

18. Content

Content of electronic software, documents, files, 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, drives etc. should follow good practice publishing standards and laws.

The following usage is not allowed:

- 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.
- Inappropriate material accidentally accessed on Internet or received via email. If this occurs, immediately leave the 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.
- Forwarding emails without permission of sender or which contain copyright material (see above note about Copyright).

19. Virus protection

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