



# DIGITAL TECHNOLOGY PROCEDURE

---

## PURPOSE

This procedure outlines the processes to ensure that all students and members of our school community understand:

- (a) our commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at school,
- (b) expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets),
- (c) the commitment to promoting safe, responsible and discerning use of digital technologies, and educating students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and digital technologies;
- (d) our policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet.

## SCOPE

This policy applies to the whole Monivae College Community.

## IMPLEMENTATION

- All staff (teaching and non-teaching) will receive training about online safety and be able to recognise and respond to online safety issues.
- Students and parents must annually sign the Acceptable use and Cybersafety Agreement each year in order to access the school's technology resources.
- Staff must annually sign the Monivae College Information Systems Usage Agreement.
- All users are to comply with the Monivae College policy and any diocesan and government legislation (such as copyright, discrimination, defamation and privacy laws) in the use of technology.
- An audit of technology use will be conducted each term or as required.
- Inappropriate material (including pornography) must not be accessed, downloaded, transmitted or posted.
- Communication and feedback between students, parents and staff via electronic media must be appropriate at all times.
- Users are expected to remain within allocated disk space and delete out of date emails and other material which take up excessive space.
- Electronic media must not be used for gambling purposes.
- Personal use for staff is restricted and limited. It must not take place during teaching or classroom time. It must not interfere with work obligations or used while supervising students (unless an emergency call to services or administration is required).
- Student and school community use is limited to educational use for engaging in student learning
- Email correspondence must contain the appropriate disclaimer.
- Users should never download or install any commercial software, shareware or freeware onto network drives or disks.
- Users should never copy other people's work or intrude into other people's files this includes logging on using the password or another user.
- Downloaded files must be checked and be virus free.



- All digital content stored and produced at or on behalf of Monivae College remains the property of the school.
- Privacy and confidentiality must be considered in forwarding or providing access to electronic communication. Permission from the sender should be sought. Staff should ensure that personal information is kept private.
- Correspondence such as email is not necessarily kept confidential when sent to an external party and can be forwarded on or accessed by others without the writer's knowledge. It is important to check whether it is appropriate to send confidential information electronically.
- Communication via chat rooms, social media email and text messages should always have appropriate content, images (if used) and language. No profane, abusive or impolite language should be used. They must not embarrass the school's reputation or be construed as bullying or harassing or embarrassing someone. (A good rule for students to follow is to never view, send or access materials which you would not want your teachers and parents to see).
- Users should ensure that their password is both secure and available to them only. It is the user's responsibility to remember their password and penalties will be incurred if the user makes a habit of returning to the administrator in this regard.
- Users should be prepared to be held accountable for their actions and for the loss of privileges if the rules of appropriate use are violated.
- Users should notify the ICT Coordinator or Network Administrator immediately if they encounter materials which violate the rules of appropriate use.
- Violation of the policy may include:
  - Informing police after an initial investigation
  - For student's restriction or suspension of use for a set period of time or in the case of a serious breach suspension from school following procedures outlined in the Monivae College Behaviour Management Policy
  - Re-imburement to Monivae College for equipment/time needed to rectify any problem caused by misuse.
  - For parents/school community- restriction or suspension of use and access for a set period. In the case of a serious breach this may be permanent.
  - For staff - informing VIT (teachers) or performance/disciplinary processes that may lead to termination of employment.
  - Regular reminders about acceptable use of technology will be communicated to staff and parents via school newsletter, staff bulletins and at staff meetings.
- Monivae College has a web filtering system in place to ensure inappropriate material cannot be accessed at school.

### **Learning and Teaching**

- The learning environment must foster student confidence to report to staff if they have seen or received anything that has made them uncomfortable or threatened. This should always be followed up in a timely manner.
- Learning and teaching practices, strategies and technologies are effectively incorporated into learning process and are used by teachers and students.
- Teachers have clear processes and practices and scaffold learning to manage classroom and online behaviour and respond appropriately to any incidents that may arise.



- Teachers provide students with an understanding of appropriate sites and materials and a process to follow if an inappropriate site/material opens.
- The school cannot filter Internet content accessed by a student from home, from other locations away from school or on mobile devices owned by students. Monivae College recommends the use of appropriate Internet filtering software on such devices.
- Teachers develop a curriculum scope and sequence for cyber safety that includes teaching safe, responsible and ethical online behaviours (see Duty of Care Policy, Anti-bullying and harassment Policy). The scope and sequence are consistent with the Victorian government requirements for curriculum (see Learning and Teaching Policy).
- Copyright and privacy laws and other legislation must not be breached in using the Internet and in posting material onto sites.
- The leadership team will monitor the cyber safety curriculum and professional learning requirements for all staff.
- Electronic teaching materials and sites used by teachers are to enhance learning and be appropriate.
- There will be regular communication to staff, students and school community on policies and procedures that foster a safe classroom environment. Information will be available on school website, Staff and Parent Handbooks. Teachers will also discuss issues and procedures with parents in informal meetings and information nights.
- Students will engage as part of their learning in using the internet which will include accessing sites such as websites, electronic chats (social media), bulletins, educational apps and classrooms and use of email.
- Teachers will provide guidance as to which sites can be accessed and programs that can be downloaded on to school devices. Teachers will develop processes for students to follow if they access an inappropriate site or are confronted with material or text that makes them uncomfortable.
- Teachers will use educational resources to develop student knowledge, skills and capabilities in cyber safety.
- Students must not post any inappropriate texts or images or engage in bullying or harassment through the use of these sites or in using email. Students must not download any unauthorised programs.
- Monivae College takes a further step towards integrating technology into the curriculum by asking all students to bring a personal IT device (Bring Your Own Device) to class for use in private study sessions and take home to follow up on classwork. This provides students the opportunity to become familiar with and develop ICT literate skills on an individual and personalised basis with the opportunity to develop essential skills needed for a connected, ethical and globalised society.
- All families receive a copy of the Acceptable Use and Cyber Safety Agreement and Bring Your Own Device (BYOD) Acceptable Use Agreement annually. Parents are asked to read the agreement with their children and sign the agreement. This is returned to the school (Refer also to Anti-bullying and Harassment Policy).

### **Mobile Phones/Electronic Devices**

- iPods, MP3s and other personal media devices are not permitted at school except as negotiated by individual subject teachers in consultations with the Director of Studies for specific educational outcomes (e.g. music and language studies). Parents will be informed of these conditions via letter for individual subjects from the subject teacher.



- Mobile phones are not to be used during school hours and are not permitted in class. They are the student's personal responsibility and must be locked in the owner's locker.
- A public phone is available for student use at recess and lunchtime.
- In an emergency, parents needing to contact their child during school hours are asked to do so by ringing the front office. We ask parents to use their discretion in this matter.
- Failure to meet these requirements will see the phone/electronic device removed from the student for two calendar weeks for the first offence.

### **School Electronic Equipment and Devices**

- Students are expected to use school equipment and devices safely and with care.
- Teachers will induct students on how to safely use and look after any electronic equipment or device.
- Students must not download programs on to school equipment or device without the permission of the teacher.

### **Social Media**

- Monivae College accepts that the use of social media is used by members of the school community as a social tool and is commonly used to express views, comments, and ideas on a range of issues.
- It is expected that no staff member is a "friend" of a student on Facebook unless a direct relative. Individual considerations may be made upon discussion with the Principal.
- It is expected that all members of the Monivae College community when in engaging with each other through using social media behave in such a manner that:
  - the welfare of all members of the school is not adversely impacted upon.
  - the reputation of the school is not negatively affected or brought into disrepute
  - personal information is kept private
  - not uploading or posting inappropriate content on any space or sight.
- Social media sites (other than those established for student learning under the supervision of a teacher) using the school name must not be established unless the principal gives permission. This permission would only be for a specific school purpose. If the site is not used appropriately according to the requirements for its use, it will be closed down.
- When using social media, it is expected that members of our school community will:
  - demonstrate appropriate personal and professional boundaries and behaviours
  - ensure online behaviour reflects the same standards of honesty, respect, and consideration that a person uses when communicating face-to-face
  - respect the rights, privacy and confidentiality of others.
  - ensure all content published is accurate and not misleading
  - not post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, threatening, violent, racist, sexist, pornographic, or is otherwise unlawful.
- not infringe on copyright or cause damage to the reputation of Monivae College or bring it into disrepute.

### **Risk Management**

The Network Administrator and ICT Committee in conjunction with the Principal will identify any risk management issues and follow the processes for risk management to ensure that risks are recorded, monitored and minimised.



**GOVERNANCE**

Supporting policies	Digital Technology Policy Duty of Care-Supervision of Students Policy Anti-Bullying and Anti-Harassment Policy Monivae College Pastoral Care Policy
Supporting schedules/forms	Acceptable Use and Cybersafety Agreement Bring Your Own Device (BYOD) Acceptable Use Agreement Staff Information Systems Usage Agreement
Associated policies	Computing and Communications Facilities Use Policy
Related Legislation	Age Discrimination Act 2004 Australian Human Rights Commission Act 1986 Disability Discrimination Act 1975 Discrimination Act 1984 Equal Opportunity Act 2010 (Victoria) Crimes Amendment (Bullying) Act 2011
Category	Operational
Approval	School Leadership Team April 2022
Endorsement	Relevant Senior Officer April 2022
Policy Owner	Compliance and Risk Manager
Date Effective	30/04/2022
Review Date	30/04/2025 (5 years from effective date)  This procedure is to be kept for three (3) years until review, unless there is a significant legislative or organisational change requiring earlier review.  The master copy is kept in Knowledge Banks in read-only in PDF form. All printed copies are uncontrolled.



Version	1.2
Content Enquiries	<a href="mailto:eguthrie@monivae.vic.edu.au">eguthrie@monivae.vic.edu.au</a>

#### DOCUMENT HISTORY

Version #	Date	Changes Made
1.0	30.04.2018	Initial release
1.1	30.04.2021	Review - Minor Content Amendments
1.2	30.04.2022	Formatting changes