Portland Secondary College

Digital Technologies Policy
(Internet, Social Medic and Digital Devices)

PURPOSE

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 including our 1-to-1 personal device program
(b) expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets, mobile phones, smart watches)
(c) the school's 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 school's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet

SCOPE

This policy applies to all students at Portland Secondary College and is part of the suite of policies which are linked to the Child Safe Policy which mandates zero tolerance of child abuse.

Staff use of technology is governed by the Department's *Acceptable Use Policy.*

DEFINITIONS

For the purpose of this policy, "digital technologies" are defined as being any networks, systems, software or hardware including electronic devices and applications which allow a user to access, receive, view, record, store, communicate, copy or send any information such as text, images, audio, or video.

POLICY

Vision for digital technology at our school

Portland Secondary College (Must Street & Victoria Parade Campuses) understands that digital technologies including the internet, apps, computers, mobile phones, smart watches and tablets provide students with rich opportunities to support learning and development in a range of ways.

Through increased access to digital technologies, students can benefit from enhanced learning that is interactive, collaborative, personalised and engaging. Digital technologies enable our students to interact with and create high quality content, resources and tools. It also enables personalised learning tailored to students' particular needs and interests and transforms assessment, reporting and feedback, driving new forms of collaboration and communication.

Portland Secondary College believes that the use of digital technologies at school allows the development of valuable skills and knowledge and prepares students to thrive in our globalised and inter-connected world. Our school's vision is to empower students to use digital technologies to reach

their personal best and fully equip them to contribute positively to society as happy, healthy young adults.

Many classes at Portland Secondary College are delivered with the use of laptops and netbooks. Students are expected to bring a charged laptop or netbook to school each day to be used during class time for different learning.

Portland Secondary College operates a Bring Your Own Device (BYOD) Program which means students must bring their own purchased netbook or laptop with them to school each day in a protective case.

Portland Secondary college does not have insurance to cover accidental damage to students' devices and parents/carers are encouraged to obtain their own insurance.

Safe and appropriate use of digital technologies

Digital technology, if not used appropriately, may present risks to users' safety or wellbeing. At Portland Secondary College, we are committed to educating all students to be safe, responsible and discerning in the use of digital technologies, equipping them with skills and knowledge to navigate the digital age.

At Portland Secondary College, we:

- use online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred
- restrict the use of digital technologies in the classroom to specific uses with targeted educational or developmental aims
- supervise and support students using digital technologies in the classroom
- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students
- have programs in place to educate our students to be promoting safe, responsible and discerning use of digital technologies.
- educate our students about digital issues such as online privacy, intellectual property and copyright, and the importance of maintaining their own privacy online
- actively educate and remind students of our *Student Wellbeing and Engagement* Policy that outlines our School's values and expected student behaviour, including online behaviours
- have an Acceptable Use Agreement outlining the expectations of students when using digital technology at school
- use clear protocols and procedures to protect students working in online spaces, which includes reviewing the safety and appropriateness of online tools and communities, removing offensive content at earliest opportunity
- educate our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies
- provide a filtered internet service to block access to inappropriate content
- refer suspected illegal online acts to the relevant law enforcement authority for investigation
- support parents and carers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home through regular updates in our newsletter and annual information sheets
- regularly monitor student traffic on the College's computer networks to identify potential problems
- audit the use of privately-owned ICT equipment such as memory sticks bought onto the school premises and school folders on the network.

Distribution of school owned devices to students and personal student use of digital technologies at school will only be permitted where students and their parents/carers have completed a signed Acceptable Use Agreement.

It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify classroom teacher or mentor as appropriate, immediately.

All messages created, sent or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and appropriate. Communications including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

Student behavioural expectations

When using digital technologies, students are expected to behave in a way that is consistent with Portland Secondary College's *Statement of Values, Student Wellbeing and Engagement* Policy, and *Bullying Prevention* Policy.

- Students must not attempt to gain entry to the system under any other user name than their own except where approved by the Information Services Manager
- Students must not attempt to delete, alter or corrupt any files other than those in their own folder
- Students are responsible for ensuring that no objectionable material is stored, displayed, downloaded or transmitted on the system. As a guide, if material stored or named would not be considered suitable for classroom display, then it is not suitable to be on the network.
- Students who bring their own personal notebooks to school are responsible for any damage and content must be appropriate to school guidelines. Any notebook which does not conform to school regulations will be confiscated and parents contacted.
- Students can expect that other students do not have access to their folder. However, staff generally and the Information Technology Manager in particular, have the right to access student folders for legitimate reasons such as supervision of the network, or class related reasons.
- If students which to introduce their own programs of any kind, it must be done with the express permission of the Information Technology Manager. Software that already exists on the network should not be copied into other locations.
- Printing is expensive. Students should use Print Preview features to check the layout of their document before printing. A spellchecker should be used before printing. Colour should only be used where required by the subject. The bare minimum printed copies should be sent to the printer. Printing is provided for curriculum purposes, not personal purposes.
- Computer rooms are to be free of food and drinks.
- Computer equipment is to be treated with respect. Physical movement in IT rooms requires care. Tampering with equipment is not permitted. Intentional damage to computers or software will result in an account for repairs and students will be banned from computer

access for a period of time at the discretion of the Information Technology Manager. Accidental damage will be dealt with at the Information Technology Manager's discretion.

When a student acts in breach of the behaviour standards of our school community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), Portland Secondary College (Must Street & Victoria Parade Campuses) will institute a staged response, consistent with our policies and the Department's *Student Engagement and Inclusion Guidelines.*

Breaches

Breaches of this policy by students can result in a number of consequences which will depend on the severity of the breach and the context of the situation. This includes:

- removal of network access privileges
- removal of email privileges
- removal of internet access privileges
- removal of printing privileges
- other consequences as outlined in the school's *Student Wellbeing and Engagement* and *Bullying Prevention* policies.
- The information Technology Manager is the adjudicator in cases of interpreting these rules, with appeal to the Principal.

SOCIAL MEDIA USE

Social media includes any online applications such as social networking sites, wikis, blogs, micro blogs, video and audio sharing sites and message boards that allow people to easily publish, share and discuss content.

Social media provides an opportunity to:

• engage and interact with our various audiences such as parents, students, staff and the wider community when used appropriately
• improve and increase staff expertise and confidence.

Maintaining professional boundaries when using social media is highly recommended. We encourage all staff when using social media to ensure that appropriate privacy filters are enabled.

The following five standards apply to employees' work use and personal use of social media at any time, when it has a clear and close connection with the department.

The department will enforce these five standards as and when appropriate:
• Always follow relevant department policies including the Code of Conduct.
• Do not act unlawfully (such as breaching copyright) when using social media.
• Make sure your personal online activities do not interfere with the performance of your job.
• Be clear that your personal views are yours, and not necessarily the views of the department.
• Do not disclose confidential information obtained through work.

Staff wishing to use social media for official department communication must gain permission from the Assistant Principal. All official communications are to be part of an overall communication plan which is monitored by the Assistant Principal.

As a matter of professional courtesy, staff will communicate with the Principal before making public comment or formal statement on educational issues or that bears on the organisation or program of the school or place of work.

The Principal will refer inquiries to the DET Media Unit, particularly if they appear to be of a potentially sensitive or controversial nature.

Official department social media accounts need to be approved by the Assistant Principal.
Formal media statements are to be made by the Principal or School Council President.

OTHER MEDIA USE

Our School Improvement Team (Principal Class Officers and Leading Teachers) and our nominated Media Liaison (Principal's Assistant) and the College Photographer will coordinate any and all media activities. Staff will seek the approval of the Principal before any contact is made with the media.

Any approaches by the media to the school or its employees for comment or information must be immediately redirected to the Principal.

A budget will be allocated for school promotion and advertising.

STAFF USE OF DET TECHNOLOGY

This Guide outlines the policy regarding the acceptable use of the Information and Communications Technology (ICT) resources of the Department of Education and Training (the Department).

The Department is responsible for ensuring the use of Department ICT resources is legal, ethical and consistent with the aims, values and objectives of the Department and its responsibilities to employees, students and other ICT users.

All users of Department ICT resources are expected to exercise responsibility, use the resources ethically, respect the rights and privacy of others and operate within the laws of the State and Commonwealth, including anti-discrimination and sexual harassment laws and the rules and policies of the Department, including occupational health and safety obligations to employees and students.

Department ICT resources should not be used for inappropriate or improper activities. This includes: pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, bullying, privacy violations and illegal activity, including illegal peer-to-peer file sharing. The audience of an electronic message may be unexpected and widespread and users should be mindful of this when using Department ICT resources.

Department ICT resources are provided to improve and enhance learning and teaching, and for the conduct of the business and functions of the Department. Using information technology, accessing information, and communicating electronically can be cost-effective, timely and efficient. Users are expected to use and manage these resources in an appropriate manner and in accordance with this policy. As part of ensuring users are aware of this policy, the following will occur:

- Users will be provided access to this policy, on HRWeb
- Users will be reminded of the need for compliance with the policy
- Users will be provided notification of updates or developments to the policy.

This section of the policy applies to all users of Department ICT resources, as defined below, located at corporate offices and schools, and in private homes or at any other location. This policy applies to all use of Department ICT resources, including, but not limited to:

- Copying, saving or distributing files
- Data
- Downloading or accessing files from the internet or other electronic sources
- Electronic bulletins/notice boards
- Electronic discussion/news groups
- Email
- File sharing
- File storage
- File transfer
- Information
- Instant messaging
- Online discussion groups and 'chat' facilities
- Printing material
- Publishing and browsing on the internet
- Social networking
- Streaming media
- Subscriptions to list servers, mailing lists or other like services
- Video conferencing
- Viewing material electronically
- Weblogs ('blogs')

Non-compliance

Non-compliance with this policy will be regarded as a serious matter and appropriate action will be taken, which may include termination of employment.
Depending on the nature of the inappropriate use of Department ICT resources, non-compliance with this policy may constitute:

- A breach of employment obligations
- A criminal offence
- A threat to the security of Department ICT resources and information
- An infringement of the privacy of staff and other persons
- Exposure to legal liability
- Serious misconduct
- Sexual harassment
- Unlawful discrimination.

Where there is a reasonable belief that illegal activity may have occurred, this may be reported to the police.

Breaches of this policy

Breaches of this policy may fall into one of the following categories, described in detail in the below table all of which brings, or has the potential to bring, the employee and/or the Department into disrepute:

- Category 1: Illegal - criminal use of material
- Category 2: Extreme - non-criminal use of material
- Category 3: Critical - offensive material.
- Category 4: Serious

Use of Department ICT Resources

Business Purposes

Department ICT resources are provided to users for business purposes. Other than limited personal use, Department ICT resources must be:

- Used for business purposes, or where authorised or required by law, or with the express permission of an Authorised Person
- Used like other business resources and users must comply with any codes of conduct, ministerial orders or legislative requirements that apply to the user, for example, the Code of Conduct for the Victorian Public Sector, the *Education and Training Reform Act 2006 (Vic)* and the *Public Administration Act 2004 (Vic)*.

Users are allowed reasonable access to electronic communications using Department ICT resources to facilitate communication between employees and their representatives, provided that use is not unlawful, offensive or otherwise improper. This may include a union on matters pertaining to the employer/employee relationship.
Large data downloads or transmissions should be minimised to ensure the performance of Department ICT resources for other users is not adversely affected.

Personal Use

Users may use Department ICT resources for personal reasons provided the use is not excessive and does not breach this policy.

Excessive personal use during working hours covers personal use which satisfies the following criteria:

- It occurs during normal working hours (but excluding an employee's lunch or other official breaks);
- It adversely affects, or could reasonably be expected to adversely affect, the performance of the employee's duties; and
- The use is not insignificant.

The Department may seek reimbursement or compensation from a user for all or part of any costs where the user has caused the Department to incur costs due to excessive downloading of non-work-related material in breach of this policy.

Subject to limited personal use, social networking, on-line conferences, discussion groups or other similar services or tools using Department ICT resources must be relevant and used only for

Department purposes or professional development activities. Users must conduct themselves professionally and appropriately when using such tools.

Unless otherwise approved, for ICT security reasons Department email addresses should not be used to subscribe to private subscriptions and other like services (e.g. on-line ticket services, bill payments) and should never be used as "recovery email' addresses for any other services. Subscribing to mailing lists and other like services using Department ICT resources must be for Department purposes or professional development reasons only and a different password must be used for all such purposes.

Users should be aware that the provisions applying to access and monitoring of Department ICT resources also apply to personal use.

Defamation

Department ICT resources must not be used to send material that defames an individual, organisation, association, company or business.

The consequences of a defamatory comment may be severe and give rise to personal and/or Department liability. Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

Copyright Infringement

The copyright material of third parties must not be used without authorisation. This includes software, database files, documentation, cartoons, articles, graphic files, music files, video files, books, text and downloaded information.

The ability to forward, distribute and share electronic messages, attachments and files greatly increases the risk of copyright infringement. Copying material to electronic storage, or printing, distributing or sharing copyright material by electronic means may give rise to personal and/or Department liability, despite the belief that the use of such material was permitted.

Users of Department ICT resources should be familiar with any relevant intellectual property and copyright guidelines issued by the Department.

For the avoidance of doubt, "copyright" does not include moral rights under the *Copyright Act 1968 (Cth)*.

Illegal Use and Material

Department ICT resources must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender may be referred to the police or other relevant authority and their employment may be terminated.

Certain inappropriate, unauthorised and non-work-related use of Department ICT resources may constitute a criminal offence under the *Crimes Act 1958* (Vic). Examples include computer 'hacking', unauthorised release of data, Department material or leaking of information or documents and the distribution of malware.

Illegal or unlawful use includes but is not limited to:

- Use of certain types of pornography under the *Crimes Act 1958* (Vic), such as child pornography
- Offences under the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic)
- Defamatory material

- Material that could constitute racial or religious vilification, or unlawfully discriminatory material
- Stalking
- Blackmail and threats under the *Crimes Act 1958* (Vic)
- Use that breaches copyright laws, fraudulent activity, computer crimes and other computer offences under the *Cybercrime Act 2001* (Cth) or *Crimes Act 1958* (Vic).
- Breaches under any other relevant legislation.

In particular, child abuse materials represent the antithesis of Department responsibilities with regard to the safety and education of children. Any suspected offender will be referred to the police and their employment will be terminated if the allegations are substantiated.

Offensive or Inappropriate Material

Use of Department ICT resources must be appropriate to a workplace environment and aligned to Department Values. This includes but is not limited to the content of all electronic communications, whether sent internally or externally.

Department ICT resources must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually-oriented messages or images and messages that could constitute sexual harassment.

All users of Department ICT resources should be familiar with Department policies including: anti-discrimination, human rights, equal opportunity and bullying and harassment.

Users of Department ICT resources who receive unsolicited, offensive or inappropriate material electronically should delete it immediately and may choose to notify their principal or immediate manager of such instances. Where the sender of this material is known to the user, the user should notify the sender to refrain from sending such material again.

Offensive or inappropriate material must not be forwarded internally or externally, or saved onto Department ICT resources, except where the material is required for the purposes of investigating a breach of Department policies.

Malware

Electronic and web communications are potential delivery systems for computer malware. An anti-virus and threat protection program should scan all data, programs and files downloaded electronically or attached to messages before being launched, opened, accessed or sent.

Malware has the potential to seriously damage Department ICT resources and lead to a breach of privacy legislation. Users should not open any attachments or click on any links embedded in an email unless they have confidence in the identity of the sender.

Social Engineering

Social engineering is (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Phishing, Vishing and Whaling and other forms of social engineering are used to obtain information from users that could result in unauthorised access to Department ICT resources, or to fraudulently obtain money from the Department.

Attribution

There is always a risk that an employee may be in breach of this policy due to false attribution. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances, an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information.

If a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. Users should inform their immediate manager or principal if they believe an electronic communication has been intercepted or modified.

Users are accountable for all use of Department ICT resources that have been made available to them for work purposes and for all use of Department ICT resources performed with their user identification. Users must maintain full supervision and physical control of Department ICT resources at all times, including mobile phones, tablets and notebook computers.

User identification and passwords must be kept secure and confidential. Users must not allow or facilitate unauthorised access to Department ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.

Active sessions are to be terminated when access is no longer required and computers secured by password when not in use.

Mass Distribution and Spam

The use of Department ICT resources for sending 'junk mail', for-profit messages, or chain letters is strictly prohibited.

The use of electronic communications for sending unsolicited commercial electronic messages ('Spam') is strictly prohibited and may constitute a breach of the *Spam Act 2003* (Cth).

Mass electronic communications should only be sent in accordance with normal Department procedures.

Confidentiality and Privacy

Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of Department ICT resources, this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

To ensure their confidentiality is maintained, employees are advised to use personal, rather than Department email accounts when disclosing improper conduct, either as part of an audit or as contemplated by the *Protected Disclosure Act 2012* (Vic).

The Department will handle any personal information collected through the use of Department ICT resources in accordance with the *Privacy and Data Protection Act 2014* (Vic).

The Department will not disclose the content of electronic communications created, sent or received using Department ICT resources to third parties outside of the Department unless that disclosure is required for the purposes of:

- A Department investigation

- A police investigation,
- For other legal, investigative, audit or compliance reasons.

In other circumstances, disclosure should not contravene the *Privacy and Data Protection Act 2014* (Vic).

Department Property

Electronic communications created, sent or received using Department email systems are the property of the Department and may be accessed by an Authorised Person or their delegate in the case of an investigation. This includes investigations following a complaint or investigations into misconduct.

Electronic communications may also be subject to discovery in litigation and criminal investigations. All information produced on users' computers, including emails, may be accessible under the *Freedom of Information Act 1982* (Vic).

Email messages may be retrieved from back-up systems.

Email Disclaimer

All emails sent externally from the eduMail service will automatically have a disclaimer attached to them.

The use of the email disclaimer may not necessarily prevent the Department or the sender of the email from being held liable for its contents.

School email systems must also append the same disclaimer to messages sent externally from the school's email service.

Access and Monitoring

Authorised Persons may access or monitor Department ICT resources at any time without notice to the user. This includes, but is not limited to, use of Department email systems, and other electronic documents and records and applies to the use of Department ICT resources for personal use. However, Authorised Persons must have a valid reason for accessing or monitoring the use of Department ICT resources and are required to maintain a log recording relevant details of the access and monitoring activity.

Authorised Persons are required to inform the Chief Information Officer (CIO), Information Management and Technology Division (IMTD) before accessing or monitoring Department ICT resources.

Authorised Persons may access or monitor the records of Department ICT resources for operational, maintenance, compliance, auditing, legal, security or investigative purposes. Electronic communications that have been sent, received or forwarded using Department ICT resources, may be accessed and logs of websites visited using Department ICT resources may be generated, examined and monitored.

Authorised Persons may require assistance of a systems administrator to gain access to records held within Department ICT resources, such as electronic documents, communications or website logs of users. In such cases, the systems administrator will not be in breach of this policy by reason of following the instructions of an Authorised Person.

If a systems administrator becomes aware of any inappropriate use of Department ICT resources, they must report their concerns to an Authorised Person.

If there is a reasonable belief that Department ICT resources are being used in breach of this policy, the principal or immediate manager of the person who is suspected of inappropriate use may secure the equipment while the suspected breach is being investigated.

The principal or immediate manager may also request the CIO to suspend a person's use of Department ICT resources.

Nothing in this policy prevents IMTD or Department agents from monitoring Department ICT resources in the normal course of their duties.

Records Management

Electronic communications are public records and subject to the provisions of the *Public Records Act 1973* (Vic).

Department record management practices must comply with Department policies and guidelines on records management and management of electronic communications, as amended from time to time. Department records may either:

- Have no retention requirement and be destroyed as soon as they are no longer required for administrative purposes.
- Be retained as a temporary record by the Department and then destroyed when the retention period designated by the Public Record Office Victoria (PROV) is complete.
- Be retained as a permanent record by the Department then, when no longer required for administrative use, transferred to PROV.

Complaints

If an employee has a complaint or report of inappropriate use of Department ICT resources, they should lodge it with the immediate manager or principal of the person who the complaint is about. If the complaint is about the employee's immediate manager or principal, they should raise it with the manager above.

Complaints arising from the use of Department ICT resources or complaints arising from the application of this policy may be investigated in accordance with Department guidelines for managing complaints, misconduct and unsatisfactory performance for the teaching service or the public service, as appropriate.

'Speak-Up' Service

Employees, contractors, and consultants are encouraged to report inappropriate conduct. If an employee has any known or suspected concerns about the appropriateness of someone's ICT use by way of an unlawful act or omission, unethical behavior, or breach of the policy, and is unable to raise it with an appropriate manager, disclosures can be made through a third-party service provider. Disclosures will be treated confidentially.

- Hotline service: 1800 633 462
- Email: educationspeakup@risqgroup.com
- Web portal: www.risqgroup/dms/educationspeakup

RELATED POLICIES, GUIDELINES AND RESOURCES

- Bullying Prevention Policy.docx
- Student Wellbeing and Engagement Policy.docx
- Inclusion and Diversity Policy.docx
- Statement of Values and School Philosophy.docx
- Student Acceptable Use Agreement
- Acceptable Use – Information and Communications Technology Resources

REQUIRED METHOD OF COMMUNICATION

- School website
- Staff induction process

RECOMMENDED PRKOFESSIONAL DEVELOPMENT

- Interactive Learning Modules – Social Media Guide
- Interactive Learning Modules – Bullying and Cyberbullying

REVIEW CYCLE

DATE	VERSION	RATIFIED BY	NEXT REVIEW
May 2021	3	Portland Secondary College School Council	May 2023