prace	**Acceptable Use of Digital Technologies Policy and Procedure**	Approval Date: 06/09/2023
		Review Date: 09/2025
		Version Number: 3.0
Authorised by:	Board	Version Date: 06/09/2023
Responsible Person:	Chief Executive Officer	
Staff Involved:	All Prace staff	

Purpose

The following policy and procedure outlines the standards and expectations for the use of Prace digital technology tools, resources and related stored information. This includes:

- acceptable use of computers, tablet devices, smart phones, email and other online tools and resources
- access to digital files and records
- maintenance of IT systems
- file management and storage.

Scope

This policy and procedure applies to Prace staff, volunteers, Board members, and contractors. It should be read in conjunction with the Prace Codes of Conduct, and the following Prace policies and procedures:

- Privacy
- Copyright
- Bullying and Harassment
- Child Safety and Wellbeing
- Social Media
- Photographing, Filming and Recording Students
- Data Breach

This policy and procedure also includes:

- the *Acceptable Use of Digital Technologies and the Internet Agreement* applicable to all Prace students and service users
- the conditions of digital technology use applicable to hirers of Prace-managed venues.

Definitions

Board means the board of the incorporated association Prace Inc, and the Prace College governing authority.

Child or young person means a person under the age of 18 years.

Child abuse includes:

a) any act committed against a child involving:
   - a sexual offence
   - grooming offences under section 49M(1) of the *Crimes Act 1958*

b) the infliction, on a child, of:
   - physical violence
   - serious emotional or psychological harm

https://www.vic.gov.au/child-safe-standards-definitions

Child safety includes matters related to protecting all children from child abuse, managing the risk of child abuse, providing support to a child at risk or child abuse, and responding to suspicions, incidents, disclosures or allegations of child abuse.

https://www.vic.gov.au/child-safe-standards-definitions

Cyber-bullying is any bullying behaviour using digital technologies that includes (but is not limited to) harassment via a mobile phone/SMS; setting up a defamatory website; comments made on social media; or deliberately excluding someone from social networking spaces.

Digital technologies means electronic tools, systems, devices and resources that generate, store or process data, including but not limited to desktop and laptop computers, tablet devices, mobile phones, software and apps, and all online tools and resources such as social media and online games. Digital learning is any type of learning that uses digital technology.

Online educational environment means online or virtual environments made available or authorised by Prace for use by students (including email, intranet systems, software applications, collaboration tools, and online services).

Prace: means the incorporated association (A0032713Z) which includes the Registered Training Organisation (4036) & Prace College (2110).

Prace College: means the section of Prace that operates as an independent school from both the Merrilands and Mernda campuses under registration number 2110.

Prace managed site means Merrilands Community Centre, Reservoir and the Prace Mernda Campus.

School governing authority, in the context of this policy and Ministerial Order 1359, means:

a) The Prace Board, including a person authorised to act for or on behalf of the Board in relation to Prace College.

b) The Principal of Prace College, as authorised by the Prace Board or the Education and Training Reform Act 2006 (Vic).

The **Senior Management Team** is made up of the Prace Chief Executive Officer (CEO), Education & Business Operations Manager, Principal of Prace College and any other staff member as appointed to the team by the CEO.

Significant child safety incident means an incident, disclosure or allegation of child abuse.

User refers to any Prace staff member, volunteer, board member, contractor student or hirer using Prace computing systems and/or facilities.

Policy Principles

Digital technologies are tools and resources that aid employees in discharging their duties, and enhance students' learning experience and engagement.

Prace digital technology resources are intended for work-related activities, learning and research. We expect all users of digital technologies at Prace or owned by Prace, to act in a safe, responsible, ethical and lawful manner, and in accordance with our Codes of Conduct.

We recognise that we have a duty of care to take reasonable steps to ensure children and young people are safe and feel safe in the educational environments we provide, including online environments. We are committed to identifying, assessing and managing risks to child safety and wellbeing in our online educational environments without compromising a child or student's right to privacy, access to information, social connections and learning opportunities.

Procedure

Guidelines for staff, volunteers and contractors in the acceptable use of digital technologies

Use of digital software

It is the policy of Prace to respect the proprietary rights of software developers. All staff, volunteers and contractors are required to comply with the licence agreements associated with the digital software products / applications ('apps') used in the course of their work with Prace, and to respect the EULA (end user licence agreement) of the developer. Permitted activities in licence agreements vary from product to product.

The following procedures must be followed:

- Individuals may not make copies or modify copyrighted software/ apps, except to the extent permitted in the licence agreement.
- Individuals may not download and/or use personally acquired software/ apps, public domain software, electronic bulletin boards or shareware without prior approval from Prace IT Technician/s.
- Software not licensed for use on a network can generally be used on a standalone basis on a computer connected to a network provided it is not used on the network. Where the licensed software is authorised for use on a network, then only the authorised number of users should use the software on the network. All such software must still be approved for use by Prace IT Technician/s.
- Acquisition of software packages must be approved by the Prace Senior Management Team. Any questions regarding the terms and conditions of copyrighted software should be referred to Prace IT Technician/s.

Use of the Prace IT network

All Prace staff, volunteers and contractors who are granted access to the local Prace IT network and/or online accounts must abide by the following at all times. This includes Prace email, cloud-based data storage systems, and any other digital software or application used by Prace.

- Making copies of system configuration files for personal use or to provide to a user external to Prace is forbidden, as is downloading or installing security programs that reveal weaknesses in systems' security.

- Individuals are not to share accounts or passwords, except when specifically delegated (e.g. an absence).

- Individuals shall not purposely engage in activity with the intent to circumvent Prace security measures or gain access to Prace systems for which proper authorisation has not been given.

- All email correspondence should be treated with the same care and diligence applied to hardcopy documentation, in accordance with the Prace *Privacy Policy and Procedure*.

- Email correspondence is to be professional in tone. Abusive, fraudulent, harassing or obscene messages and/or materials shall not be sent from, to, or stored on Prace systems. At all times, generally accepted standards of email etiquette are expected.

Use of the Internet

Prace recognises that the Internet is an essential tool to aid workers in discharging their duties. As such, its primary use is to be for work-related purposes, including education, research, communication, and administration as applicable to Prace business objectives. Understanding that all activities on the Internet may be traced back to Prace, work on the Internet shall be conducted in such manner that public confidence and trust in the integrity, objectivity and professionalism of Prace is conserved and enhanced.

- No Prace information shall be made available for public access without approval of senior management.

- Non-work-related activity on the Internet, including email and the use of social networking sites such as Facebook, shall be conducted on an individual's own time, outside of regular hours of work. During this time, these guidelines remain in force.

- Under no circumstances is it appropriate, at any time, to peruse inappropriate websites, post inappropriate messages, or send inappropriate e-mail correspondence. The term "inappropriate" includes, but is not limited to, sites/subjects that advocate principles or beliefs not in keeping with Prace Codes of Conduct and Values, sites/subjects that advocate illegal activities and sites/subjects that are sexual/pornographic in nature.

- Where, for legitimate research purposes, a user wishes to access a site or deal with a subject that may be considered prohibited, it must be discussed in advance, and approved, by their direct supervisor who, if in doubt, will raise it with Prace senior management. At any time, Prace reserves the right to monitor computer activities, including Internet usage among its users.

- All staff, volunteers and contractors are required to abide by the Prace *Social Media Policy*, which sets out expectations in relation to both professional and personal use of social media, and when making public comments online.

Online services and applications

When Prace is considering using a new online service or application that handles personal information, staff members must:

1. Conduct an assessment to identify any privacy and security risks, and document actions required to mitigate these. Refer to *Work Instruction - Privacy Impact Assessment for Remote Learning Services and Applications*

2. Consider whether consent for use of the service is required, and if so, whether opt-in or opt-out consent is most appropriate for the specific situation.

3. For Prace College students ensure parents/carers are adequately informed about the use of the online service.

Privacy in online environments

In accordance with the Prace *Privacy Policy and Procedure*, staff, volunteers and contractors must take reasonable steps to ensure that personal and health information they create, handle or have responsibility for is kept secure at all times, and that they only collect, use, disclose, and dispose of it appropriately and lawfully.

The Prace *Social Media Policy* and *Photographing, Filming and Recording Students Policy* also contain privacy protection requirements that must be followed by all staff, volunteers and contractors.

Unauthorised disclosure or access to Prace IT systems, including online accounts or data, is strictly prohibited. Security breaches must be reported immediately to the line manager, and the *Data Breach Response Policy and Procedure* must be followed to determine if the security breach has resulted in a notifiable data breach.

Access to computer files

Employees issued with a computer login and password must not share these details with anyone under any circumstances, either internal or external to Prace. If a password has been compromised, IT Technician/s must be informed to have the password reset.

The above guidelines concerning Internet usage shall apply at all times while utilising Prace IT systems and digital technologies. Failure to comply with the above guidelines may result in disciplinary action up to and including termination of employment/engagement. Illegal activity may be prosecuted.

Maintenance of computer systems

All necessary precautions are to be taken to maintain and protect the organisation's IT systems, such as virus control measures, regular maintenance, and updating of all computer hardware and software. No unauthorised software is to be loaded onto Prace computers. All reasonable security measures are to be taken to ensure the

safety of computer and associated equipment. Prace employs IT Technician/s to ensure the safety and security of all electronic files.

Unlawful activity

Any suspected illegal online acts are to be reported to the Senior Management Team and will be referred to the relevant law enforcement authority for investigation.

Guidelines for the use of digital technologies for teaching and learning

Digital technologies and the Internet provide opportunities to enhance students' learning experience and engagement. Prace computers, digital devices and internet resources are intended for learning and research. Responsible use of these resources by students, with guidance from teaching staff, will provide a secure and safe learning environment.

Teachers/trainers should also refer to the Prace *Social Media Policy* for specific expectations and requirements in relation to social media use in the context of teaching and learning.

Acceptable Use of Digital Technologies and the Internet Agreement

At Prace we support the right of all members of the Prace community to access safe and inclusive learning environments, including digital and online spaces. The following agreement outlines the expected behaviours we have of our students and service users when using digital technologies or online content.

General Principles:

1. Prace may provide access to digital technologies, including digital devices and Wi-Fi / Internet, during class hours, for students to develop their learning.
2. Prace may also provide access to digital technologies and the Internet outside of class times, for students to complete coursework. This may be at a Prace managed site, an external venue, or at home.
3. At Prace we have a **Student Code of Conduct** that outlines our values and expected standards of student conduct. We expect all students to use digital technologies and the Internet responsibly, efficiently, ethically and legally.

Upon enrolment students sign an "Acceptable Use of Digital Technologies and the Internet Agreement" in which students agree to abide by the following.

Student Declaration:

When I use digital technologies and Wi-Fi / Internet during class hours, or use digital technologies provided by Prace **at any time**, I have responsibilities and rules to follow.

I agree to:

1. **Use the Internet only for study and learning**

   as directed by the teacher and for the purposes of meeting course learning requirements. This includes:

   - Not downloading unauthorised programs, including games
   - Not interfering with network systems and security or the data of another user
   - Not attempting to log into the network or online service with a username or password of another person
   - Being mindful of the content I upload or post online, ensuring all material is appropriate and in line with the values outlined in the *Student Code of Conduct.*

2. **Stay within the law and use the Internet legally**

   This includes laws covering copyright, intellectual property, spam, privacy, discrimination, telecommunications, broadcasting, criminal law, freedom of information, human rights and equal opportunity.

3. **Protect my own privacy**

   By not giving out personal details, such as my full name, telephone number, address, passwords and images.

4. **Protect other people's privacy**

   By not posting or forwarding the personal details, information, images or recordings of others without their consent.

5. **Obtain consent before photographing/recording others**

   This includes only taking photographs or sound or video recordings when others are aware the recording is taking place and have provided their explicit consent as part of an approved learning activity.

6. **Not share Zoom/Google Meet Links**

   I will protect the privacy and security of Prace students and staff by not sharing or posting the link to a video conferencing meeting with others, offline in public communications or online on public websites or social media forums.

7. **Never steal other people's work**

   I will use the Internet in a manner that does not infringe copyright or intellectual property rights; including not distributing or sharing content (such as music and other audio materials and video materials) or software. I will abide by copyright and intellectual property regulations by attributing references appropriately, and by requesting permission to use images, text, audio and video.

8. **Never steal anyone's identity**

   I will never intentionally use another person's credentials, or impersonate or falsely represent myself as another person.

9. **Treat other people ethically and with respect**

   This includes communicating with others in a supportive and respectful manner, and never harassing, bullying, threatening, defaming, vilifying or sexually harassing anyone. I will not participate in online bullying (e.g.

forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours).

10. **Keep it clean - stay away from any kind of obscene or offensive material**
    I will not use digital technologies to create, transmit, access, look for, publish or store electronic material that is obscene, offensive or inappropriate.

11. **Handle all equipment with care**
    I will notify my teacher if any damage occurs, or if something needs attention. I won't install any software without express permission.

12. **Be 'cyber-safe'**
    I will speak with a teacher or trusted adult if I feel uncomfortable or unsafe online, or if I see others participating in unsafe, inappropriate or hurtful online behaviour.

The misuse of digital technologies and the internet may result in disciplinary action in accordance with the *Student and Service Users Disciplinary Policy and Procedure* and/or *Student Behaviour Management (Prace College) Policy and Procedure*.

Teachers/Trainers will ensure that:

- Any problems with Prace digital resources or equipment are reported to Prace IT Technician/s
- Any student found accessing any material that is fraudulent, discriminatory, threatening, bullying, racist, sexually explicit or otherwise inappropriate or unlawful is reported to Prace management
- Anyone found performing malicious activities is reported to Prace management
- Anyone found wilfully damaging computer or computer related equipment, is reported to Prace management

Prace College Duty of Care

Prace College has a duty of care to take reasonable steps to ensure its educational environments promote safety and wellbeing while minimising the opportunity for young people to be harmed. This includes ensuring digital learning is conducted in a safe and responsible manner.

As part of its annual risk management processes, the online environments used by the College as part of the education program are to be reviewed and evaluated in relation to child safety, and strategies developed to mitigate any identified risks. This will be added to the Prace risk register, which is reviewed and approved by the Board annually. Such strategies must aim to minimise risk without compromising the students' right to privacy, access to information, social connections or learning opportunities.

In addition to the guidelines for teachers and students set out above, the following directions specific to Prace College operations must be adhered to.

- **Supervision**

  Teachers must ensure that students are adequately supervised and supported when using digital technology in the classroom and when engaged in online learning.

  Parents and/or carers must be informed of the learning spaces made available to students as well as the expected behaviours and protocols surrounding their use. All students must sign and adhere to the *Acceptable Use of Digital Technologies and the Internet Agreement*.

- **Information privacy**

  In accordance with the Prace *Photographing, Filming and Recording Students Policy*, images or recordings of students are not to be made publicly available without the express consent of the student and their parent.

- **Cyber-safety education**

  Schools have a responsibility to educate young people about responsible online behaviour. Online safety education is included within the school's curriculum planning and taught explicitly.

- **Responding to online incidents**

  The College has a duty of care to respond to any incident brought to the attention of the College that impacts on a student or other students within the College environment, and/or impacts on the College's operations, regardless of when and where the incident occurred.

  Where such an incident involves the behaviour of a Prace College student in an online environment, the College will respond in accordance with the Department of Education's *Step-by-Step Guide: Responding to online incidents of inappropriate behaviour by students*, along with the following Prace policies and procedures (as applicable depending on the nature of the incident).

  - *Student Behaviour Management (Prace College) Policy and Procedure*
  - *Bullying and Harassment Policy and Procedure*
  - *Data Breach Response Policy and Procedure*
  - *Child Safety Reporting Procedure*
  - *Child Safety and Wellbeing Policy*
  - *Critical Incidents Policy and Procedure.*

Hirers of Prace-managed venues

The following terms are to be incorporated into the Conditions of Hire for Prace-managed venues:

Hirers must abide by the following Prace Wi-Fi / internet conditions of use. Hirers will:

- Use the internet lawfully, including within laws relating to copyright, intellectual property, spam, privacy, discrimination, telecommunications, broadcasting, criminal law, human rights and equal opportunity
- Not create, transmit, access, look for, publish or store electronic material that is obscene, offensive or inappropriate.

	• Handle all equipment with care, and notify the Facilities Coordinator if any damage occurs, or if something needs attention.
Review	This Policy and Procedure will be reviewed every two years, and after any significant child safety incident or complaint, or in response to significant emerging risks or further government mandates/requirements. The Prace Board is responsible for reviewing and approving this Policy and Procedure.
Glossary	IT – Information Technology
Relevant Legislation / Standards	Child Safe Standards (Vic) Child Safety and Wellbeing Act 2005 (Vic) Copyright Act 1968 (Cth) Ministerial Order 1359 (Child Safe Standards) Online Safety Act 2021 (Vic) Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) Privacy and Data Protection Act 2014 (Vic) Privacy Act 1988 (Cth) Record keeping requirements AQTF Standards
Related Policies and Procedures	Bullying and Harassment Policy and Procedure Child Safety and Wellbeing Policy Child Safety Code of Conduct Child Safety Reporting Procedure Copyright Policy and Procedure Data Breach Response Policy and Procedure Photographing, Filming and Recording Students Policy Privacy Policy and Procedure Records Management Policy and Procedure Risk Management Policy and Procedure Social Media Policy Staff Disciplinary Policy and Procedure Staff, Volunteers and Contractors Code of Conduct Student Behaviour Management (Prace College) Policy and Procedure Student Code of Conduct Student and Service Users Disciplinary Procedure Volunteer Policy and Procedure
Related Documents	Acceptable Use of Digital Technologies and the Internet Agreement New MCC Booking Application Form – Conditions of Hire
Consultation	Prace College Principal Prace College Subcommittee Prace Board Senior Management Team Compliance Manager