prace	**Acceptable Use of Digital Technologies Policy and Procedure**	Approval Date: 07/10/2021
		Review Date: 10/2024
		Version Number: 2.0
Authorised by:	Executive Officer	Version Date: 07/10/2021
Responsible Person:	Executive Officer	
Staff Involved:	All Prace staff	

Purpose

The following outlines acceptable standards for the use of Prace computing systems, facilities and related stored information, including:

- acceptable use of computers, Internet, email and social networking sites
- access to computer files
- maintenance of computer systems
- file management and storage

Scope

This policy applies to all users of Prace computing systems and facilities, including Prace Staff, volunteers, Board members, contractors, students and hirers.

Relevant Legislation / Standards

Copyright Act 1968 (Cth)
Privacy and Data Protection Act 2014 (Vic)
Privacy Act 1988 (Cth)
Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

Record keeping requirements AQTF Standards

Definitions

Cyber-bullying is any bullying behaviours 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: Digital technologies are **electronic tools, systems, devices and resources that generate, store or process data**. Well known examples include social media, online games, multimedia and mobile phones. Digital learning is any type of learning that uses technology.

Prace: means the incorporated association (A0032713Z) which includes the Registered Training Organisation (4036) & Prace College (022110).

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.

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

Policy Principles

Computers and the internet provide opportunities to aid employees in discharging their duties and enhance students' learning experience and engagement.

Prace computers and internet resources are intended for work-related activities, learning and research. We expect all users accessing computer facilities at Prace or owned by Prace, to do so in a responsible, ethical and lawful manner.

Procedure

Guidelines for Staff in the Acceptable Use of Digital Technologies

Use of computers- software

It is the policy of Prace to respect the proprietary rights of a computer software developer. As a user, you are required to comply with the licence agreements associated with the computer software products and to respect the EULA (end user licence agreement) of the software 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, except to the extent permitted in the licence agreement.
- Individuals may not download and/or use personally acquired software, public domain software, electronic bulletin boards or shareware without prior approval from Prace IT Technician/s
- Software which is not licensed for use on a network can generally be used on a standalone basis on a computer which is connected to a network as long as it is not used on the network. Where the licensed software is authorized for use on a network, then only the authorized number of users should use the software on the network. All such software should still be approved for use by Prace IT Technician/s
- Acquisition of software packages must be approved by Prace senior management. Any questions regarding the terms and conditions of copyrighted software should be referred to Prace IT Technician/s.

Use of Email

Prace supports an E-mail network for work-related correspondence among people who have accounts.

- E-mail correspondence, at all times, will 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 e-mail etiquette are expected.
- 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, passwords or dial-up modem telephone numbers, 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 e-mail correspondence should be treated with the same care and diligence applied to hardcopy documentation.

Use of the internet

Prace recognizes that the Internet is a useful tool to aid employees in discharging their duties. As such, its primary use is for education, research, communication and administration as applicable to Prace business. 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 e-mail 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 web sites, 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's *Code 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 her/his 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.
- **Social Networking sites:** Employees are cautioned about posting messages or information that refer to work, work related matters or fellow colleagues on social networking sites that may not be appropriate or which may be deemed offensive. Refer to Prace's *Social Media Policy* and *Bullying and Harassment Policy and Procedure*.

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 what actions are 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. And for Prace College students ensure parents/carers are adequately informed about the use of the online service.

Privacy in online environments
Staff are to be mindful and take must take reasonable steps to ensure that personal and health information they create, handle or have responsibility for are kept secure at all times, and only collect, use and disclose it in appropriate ways.

Breach of security or materials is strictly prohibited at Prace or anywhere else. Security breaches must be reported immediately to the line manager. At all times the above guidelines concerning Internet usage shall apply while utilising Prace's computer system. Where there is a data breach please apply the *Data Breach Response Policy and Procedure*.

Failure to comply with the above-mentioned policy may result in disciplinary action up to and including termination of employment. Illegal activity may be prosecuted.

Access to Computer Files:
Employees issued with a computer login and password should under no circumstances share these details with anyone, either internal or external to Prace. If a password has been compromised, IT Technician/s must be informed to have the password reset.

Maintenance of Computer Systems:
All necessary precautions are to be taken to protect the organization from computer failure, such as virus control measures, regular maintenance and updating of all computer hardware and software. No illegal 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 Teachers, Trainers and Students in the Use 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.

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. This 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.

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**
   Laws about the Internet may focus on these areas: copyright, intellectual property, spam, privacy, discrimination, telecommunications, broadcasting, criminal law, freedom of information, human rights and equal opportunity.

3. **Protect my own privacy**
   Do not give out personal details, including my full name, telephone number, address, passwords and images;

4. **Protect other people's confidence or secrets or privacy**
   Do not post or forward the personal details, information or images of others without their consent.

5. **Obtaining consent to record others**
   Only taking and sharing 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 lesson.

6. **Not Sharing College Zoom/Google Meet Links**
   Protecting the privacy and security of my school community 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**
   Use the Internet in a manner that does not infringe copyright or intellectual property rights; including not distributing, sharing, content (such as music and other audio materials and video materials) or software. Abide by copyright and intellectual property regulations by requesting permission to use images, text, audio and video, and attributing references appropriately.

8. **Never steal anyone's identity**
   Do not intentionally use another person's credentials, or impersonate or falsely represent yourself as another person.

9. **Treat other people ethically and with respect**
   Don't harass people. Don't bully, threaten, defame, vilify or sexually harass them.

10. **Keep it clean - stay away from any kind of obscene or offensive material**
    Don't 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**
    Notify your teacher if any damage occurs, or if something needs attention. Please don't install any software without express permission.

12. **Cyber-Safety**
    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 computers 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 are reported to management
- anyone found performing malicious activities are reported to management
- anyone found wilfully damaging computer or computer related equipment, are reported to management

Prace College

The College has a duty of care to students to take reasonable steps to ensure digital learning is conducted in a safe and responsible manner.

In addition to the above guidelines, 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. The College has its own *Acceptable Use of Digital Technologies and the Internet Agreement* which all students must sign and adhere to.

- Posting personal details or photographs of Prace College students in any forum outside the College and accessible to the public is prohibited.

- Cyber-safety education -The College has a duty of care to students to take reasonable steps to ensure digital learning is conducted in a safe and responsible manner and that students are educated about responsible online behaviour and safety.

  Online safety education is included within the school's curriculum planning and taught explicitly.

- Responding to online incidents - The misuse of digital technologies and the internet will be dealt in accordance with the *Student Behaviour Management (Prace College) Policy and Procedure* and/or *Student and Service Users Disciplinary Policy and Procedure.*

  For incidents that occur outside of class hours, a behaviour management and/or disciplinary response should only be implemented where it impacts on a student's ability to successfully participate during class. E.g. A student is cyber-bullying another student outside of class hours. The victim is impacted and cannot engage in their studies. This out-of-school behaviour can then be addressed with a behaviour management or disciplinary response as appropriate.

	See the Prace *Bullying and Harassment Policy and Procedure* for specific response to instances of cyberbullying.
Glossary	IT – Information Technology
Related Policies and Procedures	Acceptable Use of Digital Technologies and the Internet Agreement Data Breach Response Policy and Procedure Bullying and Harassment Policy and Procedure Privacy Policy Records Management Policy & Procedure Risk Management Policy & Procedure Social Media Policy Staff Disciplinary Procedure Student Behaviour Management (Prace College) Policy and Procedure Student Code of Conduct Student Disciplinary Procedure