

STUDENTS ONLINE GUIDELINES AND PROCEDURES

RATIONALE

Perth Modern School provides online services to students for learning-related activities and makes every reasonable effort to educate and protect students from exposure to inappropriate online material and activities.

The school recognises access to online resources in and out of school gives students greater opportunities to learn, engage, communicate, build community spirit, and develop skills that will prepare them for work and life. We will provide appropriate supervision for students using online services for learning-related activities on the school site and take appropriate action in accordance with the Student Behaviours in Public Schools Policy when there is a breach of the Acceptable Usage Agreement.

IMPLEMENTATION AND COMPLIANCE

The Principal and School Administrators are responsible for implementing the Department of Education Students Online in Public Schools Policy.

Line Mangers (Heads of Learning Area and Program Coordinators) are responsible for compliance monitoring and will communicate the requirements of the Students Online in Public Schools policy and procedures to any teachers involved with the provision of online services for learning-related activities. This includes:

- Educating students about the risks and their responsibilities accessing the Department's online services and associated online activities.
- The school providing and maintaining student passwords in accordance with the Cyber Security policy.
- Enabling students to bring their own device to school through Personally Owned Devices (POD) or Bring Your Own Device (BYOD) to access software and applications through the Department of Education's network.
- Not excluding students who do not have a POD or BYOD from any part of the educational program.
- Confirming that permission to publish work or images of students has been received.

SCHOOL ACCEPTABLE USAGE AGREEMENT

All students are required to read and sign (with a parent countersignature) the School's Acceptable Usage Agreement. This document sets out the permission for the school to access and monitor usage through the school Online environment and the school's ability to access POD and BYOD to determine compliance with the policy where necessary. This agreement will be completed via the online Enrolment Form.

Access to Department online services will be granted to students after receiving an Acceptable Use Agreement signed by the student and/or parent (for students under 18 years of age) or by the student (18 years and older).

Department services include, but are not limited to, email, calendar, instant messaging, web conferencing, discussion groups, online file sharing and storage, learning management systems, internet access and web browsing that may be accessed using the computer networks and services of the Department.

PERSONAL INFORMATION, PRIVACY AND CONFIDENTIALITY

The school encourages parents/carers/guardians to be vigilant in their supervision of the use of online services by their children and will keep parents informed of issues if they arise. Students can access a number of internet sites that provide advice regarding cyber-safety, eg. the Australian Government's Cybersafe web page.

In supporting the safe use of Information Communication Technologies (ICT) and online services the school will ensure:

- An education program regarding cyber-safety is available to parents and students. This helps to ensure that all students are regularly reminded of the issues and responsibilities associated with ICT in the school and the wider community.
- A level of content filtering that blocks sites based on category. Blocks are applied to sites that have been identified as unsuitable for the education market.
- Staff monitor students' online resources in classes.
- With regards to emails, staff and students are required to use the Department of Education email system when emailing with each other.

By educating students of the risks associated with any online activities and how to adopt protective online behaviour to avoid exposure to inappropriate online content or activities student behaviours should include:

- Understanding their rights as a child for safety, respect and privacy.
- Identifying behaviours online from adults or students which are inappropriate or unsafe.
- Seeking help from people within their trusted adult network.
- Knowing where to find support when they are being cyberbullied or receiving unwanted contact.
- Using appropriate practices for the physical and logical storage and security of digital information such as not storing private information on public websites.
- Applying appropriate protocols when using ICT to safely create, communicate or share information such as posting to social media.
- Never publishing or disclosing the email address of a staff member or student without that person's explicit permission.
- Taking care when revealing personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- The risks associated with any online activities and how to adopt protective online behaviour to avoid exposure to inappropriate online content or activities.

PERSONALLY OWNED DEVICES (POD) AND BRING YOUR OWN DEVICE (BYOD)

Appropriate use of devices can enhance the educational experience for students and aid learning. When used appropriately devices offer students and parents' advantages in terms of ease of communication and personal safety after school hours. The Student Mobile Phones in Public Schools Policy bans students from using mobile phones from the time they enter school grounds to the conclusion of the school day, and requires students to put their smart watches in 'airplane mode'.

Expectation of Students

- Users of devices are expected to display courtesy, consideration and respect for others whenever they are using such a POD or BYOD.
- Devices should not be used in any manner or place that is disruptive to the normal routines of the school or to other people.
- Devices for classroom use must be brought to school fully charged and in working order.
- Before arriving on campus mobile phones and ear buds/headphones, must be switched off and away until the student departs the campus at the end of the school day.
- Mobile phones and earbuds/headphones may be used under the instruction of the teacher for a specific educational purpose.
- Smart watches are to be placed in 'airplane mode' so phone calls and messages cannot be sent or received during the school day.
- The use of a device and its embedded camera or video recording may only occur with the express permission and supervision of the classroom teacher for curriculum purposes.
- Using cameras without the knowledge and/or permission of those being filmed is an invasion of privacy and is not permitted.
- Gaming during school time is not permitted.

CONSEQUENCES OF MISUSE

The school will determine whether inappropriate use of devices or online services has occurred and act in accordance with the Student Behaviour Policy where there is a breach of acceptable use. Where there is a serious breach of this policy, which is potentially criminal in nature, the Police will be notified.

Reporting Misuse

In the first instance approach a parent, staff member or the Associate Principal Student Services.

If you make a mistake:

- Be sure to correct any mistake you make immediately and make it clear what you have done to fix it.
- Apologise for the mistake if the situation warrants it.
- If it is a significant mistake (eg. exposing private information or reporting confidential information), please let the Associate Principal Student Services know as soon as possible so the school can take the proper steps to help minimise the impact it may have.

Misuse of Devices

The student who owns the device will be held responsible for its use.

Any breaches of this policy will result in the device being confiscated and delivered to the Program Coordinator Student Services Manager. Students will need to see the Program Coordinator Student Services to collect the device at the end of the day.

For serious breaches of this policy, parents will be notified, and they will need to collect the device from the Associate Principal Student Services. The Police may be notified.

RELATED DEPARTMENT POLICIES

[Child Protection in Department of Education Sites](#)

[Duty of Care for Public School Students](#)

[Incident Management on Department of Education Sites](#)

[Cyber Security](#)

[Intellectual Property](#)

[Student Behaviour in Public Schools](#)

[Software Use](#)

[Telecommunications Use](#)

[Students Online in Public Schools](#)

[Student Mobile Phones in Public Schools](#)