



Department of  
**Education**

# **Students Online in Public Schools Procedures**

Effective date: 19 March 2019

Version: 3.5

Last update date: 3 March 2023

These procedures must be read in conjunction with the Students Online in Public Schools Policy.

## Table of contents

<b>1. Policy supported</b>	<b>3</b>
<b>2. Scope</b>	<b>3</b>
<b>3. Procedures</b>	<b>3</b>
3.1 Consent and acceptable use agreements	3
3.2 Student personal security	4
3.3 Responsible online practice	4
3.3.1 Personal information, privacy and confidentiality	4
3.3.2 Publishing student images and information	5
3.4 Third party service providers of online applications	6
3.5 Student misuse and breach of acceptable use	7
3.5.1 Receiving inappropriate material from students	8
<b>4. Definitions</b>	<b>8</b>
<b>5. Related documents</b>	<b>10</b>
<b>6. Contact information</b>	<b>12</b>
<b>7. History of changes</b>	<b>12</b>
<b>8. Appendices</b>	<b>14</b>
<b>9. More information</b>	<b>15</b>
Procedure review date	15
Procedure last updated	15

**These procedures must be read in conjunction with the Students Online in Public Schools Policy.**

## 1. Policy supported

Students Online in Public Schools Policy

## 2. Scope

These procedures apply to Site Managers.

## 3. Procedures

### 3.1 Consent and acceptable use agreements

Site Managers must confirm that every student has signed parental permission to have an Online Services account and Acceptable Use Agreement to access Department provided services.

#### **Guidance**

A Sample Letter to Parents (Appendix A) and Permission for Students to have an Online Services Account (Appendix B) are provided as templates.

The sample Online Services Acceptable Use Agreements are written for three phases of schooling: K-2 (Appendix C); 3-6 (Appendix D) and 7-12 (Appendix E) and change in complexity and detail.

These documents can be modified to include school logos and additional school-related information where schools have their own licences for online services.

Note as online services continue to grow, it is recommended that agreements be reviewed regularly.

#### **Logon reminder notice**

The notice below should be displayed to all students when accessing the internet through the Department's network.

"Appropriate Use of Online Services

When using any of the WA Department of Education's online services you agree;

- to the rules set out in the Acceptable Use Agreement

- to give consent to the Department monitoring these services
- that any misuse of these services could result in disciplinary action.”

## 3.2 Student personal security

Site Managers must confirm all staff involved with learning related online services have taken adequate steps to educate students about applying personal security protocols such as keeping passwords secure in an online environment.

### Guidance

Refer to the Department Account Manager (DAM) for the [Student User Guide \(staff only\)](#).

Note when resetting students' passwords in DAM tick the forced change at next logon box. Students will be directed to make the change at their next login.

Student passwords can also be managed by classroom teachers in Connect. In this instance teachers need to remind students when logging into Connect to change their password in My Connect.

## 3.3 Responsible online practice

Site Managers must confirm that staff involved with learning related online services are kept up to date with the relative risks and educational benefits of online activity by their students.

### Guidance

[The Australian Government's Office of the eSafety Commissioner](#) provides information and resources to support safe, positive experiences for young people online

Information is also available from [Access resources for online safety](#) in Ikon (staff only)

### Content filtering

The Department of Education provides a level of content filtering that blocks sites based on category.

Note blocks are applied to sites that have been identified as unsuitable for the education market. Many schools also operate local filtering systems to block sites deemed inappropriate for their school in an endeavour to reduce the risk of student exposure to inappropriate content.

Schools wishing to have further sites blocked at a system level should contact the Customer Service Centre (CSC) on 9264 5555 or [raise a request](#).

### 3.3.1 Personal information, privacy and confidentiality

Site Managers must confirm that staff have educated 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.

### **Guidance**

Such behaviours could 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; and
- taking care when revealing personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.

Further information and resources can be found on the website of the [Office of the eSafety Commissioner](#) and [Access resources for online safety](#) in Ikon (staff only).

### **3.3.2 Publishing student images and information**

Site Managers must:

- confirm that permission to publish work or images of students has been received; and
- approve any material planned for publication on the internet or intranets and confirm it has appropriate copyright and privacy clearance.

### **Guidance**

Identifying information that accompanies published student images on the internet should be limited.

Only use photos of students in regular school uniform or day clothing when publishing on the school's intranet or internet.

A sample letter Permission to Publish Student Images and Work for School Purposes (Appendix F) is provided as a template.

Refer to the Intellectual Property Policy and Procedures and Copyright for Schools Guidelines

Note photographs of single students (except where receiving an award or similar) and of students in swimming costumes or similar clothing should be avoided (for example this applies to images in school newsletters, school handbooks).

For further information on the specific requirements regarding students in the care of the Department of Communities Chief Executive Officer refer to Section 10 Consent for publications, photographs and school activities in the [Memorandum of Understanding between the Department of Communities and the Department of Education 2021 \(staff only\)](#).

### 3.4 Third party service providers of online applications

Site Manager must assess the risk of the Third Party Service Provider.

#### Guidance

The site manager is responsible for confirming that a risk assessment of the online third party service provider has been completed and that the third party service meets a genuine teaching and learning, administration or communication need.

Online third party services often require separate account creation and login credentials, and provide content, activities or transactions via the internet. These services often require schools to provide personal information of student and/or parents.

Site managers should:

- identify third party services which hold personal information for students;
- check the Third Party Services Catalogue on Ikon (staff only) for an appropriate online service. Review the risk assessment of the [Third Party Service Provider](#) (staff only) and manage online third party services at your school;
- implement the appropriate notification or consent option for an individual or their parent as specified in the Third Party Service Risk Report;
- implement actionable treatments from the Risk Assessment Report for the chosen online services; and
- implement an annual (or ad-hoc if required) parental notification/consent process with provisions to opt-out from using specific applications.

If a required online service is not included in the Third Party Services Catalogue, request an online service risk assessment by [Raising a Request](#).

An Online Third Party Service – Parent Letter (Appendix G) outlines how third party services are used in schools and the need for parent consent for some third party services.

Provide this parent letter alongside the Online Third Party Services – Parent Notification Form (Appendix H) and/or Online Third Party Services – Parent Consent and Agreement Form (Appendix I). Appendix I has the opt-out option and includes an optional verbal consent template. This information can be given to parents in hardcopy or electronic formats. Schools can provide a list of online services directly to parents or publish a list of the online services on the school website.

Risk assessment and consent are not required for Department-provided online services or services that do not collect personal information.

Information regarding [translation](#) and [interpreting](#) services to assist schools in communicating this information to parents can be found on Ikon (staff only).

Third party online services are those provided by an external organisation, consultant or independent contractor and may be free or paid. Examples of education specific Third Party Service Providers include applications such as Google Apps for Education, Seesaw, Studyladder, Skoolbag, Reading Eggs, Mathletics, and ClassDojo. Third party services may be accessed via websites or downloaded from retailers such as Apple iTunes, Google Play and Office365. Third party social media services, which may also hold personal information, could include Facebook, Instagram and Twitter.

### 3.5 Student misuse and breach of acceptable use

Site Managers will take appropriate action in accordance with the [Student Behaviour in Public Schools Policy and Procedures](#), [Child Protection in Department of Education Sites Policy and Procedures](#) and the school's Behaviour Management Plan where there is an alleged misuse of online services or breach of acceptable use.

#### Guidance

Site Managers and staff should:

- follow procedures for fairness and due process where there is an alleged misuse or breach of acceptable use, for example by investigating any reported misuse and, where possible, accurately retracing misuse to the offender;
- seek further clarification from [Child Protection in Department of Education Sites Procedures for Principals](#), [Child Protection in Department of Education Site Procedures for Teachers](#) and [Respond to a student disclosure of abuse](#) in Ikon (staff only) if the matter requires support from the Department of Communities.
- tailor disciplinary action taken in relation to students to meet specific concerns related to the breach (for example counselling, parental involvement, police involvement), and assist students in gaining the self-

discipline necessary to behave appropriately when using the online services; and

- promptly address inappropriate online/social media posts that are either defamatory, misrepresent the school and its intellectual property, display objectionable content or incite violence or threaten the safety of students or staff. Site Managers and staff should keep a record of the nature and the location of the offensive inappropriate content and block, unfollow or hide people and inappropriate posts that appear on your school's page or feed. Refer to the [Office of the eSafety Commissioner](#).

When sexually explicit or child exploitation material has been located on a student's mobile phone or electronic device or if sexually explicit or child exploitation material has been or is alleged to have been distributed to others, site managers and staff should refer to the relevant procedure in the [Child Protection in Department of Education Sites policy and procedures](#).

To access more information, refer to [Escalate inappropriate social media content \(staff only\)](#) and [Report sexually explicit or child exploitation material \(staff only\)](#).

### 3.5.1 Receiving inappropriate material from students

Site Managers must communicate to teaching staff the steps to take and advice to give, if students notify them of inappropriate or unwelcome online activity by fellow students or members of the public.

#### Guidance

Refer to [Child Protection in Department of Education Sites Procedures for Principals](#) and for teachers [Child Protection in Department of Education Site Procedures for Teachers](#).

## 4. Definitions

### Department-provided online services

Department services including, but 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.

### Inappropriate content

Content that is considered unsuitable or harmful to students. It includes material that is pornographic, racist, sexist, inflammatory, threatening, hateful, obscene or abusive in nature or which promotes or encourages illegal activities or violence. For specific definitions regarding child exploitation material including child pornography and sexting refer to the [Child Protection in Department of Education Sites](#) policy.

### **Learning-related activities**

School activities that are part of the planned class and/or whole school education of a child.

### **Parent**

In relation to a child, a person who at law has responsibility for the long term care, welfare and development of the child; or the day-to-day care, welfare and development of the child.

### **Teaching staff/residential college and camp school staff**

Persons appointed by the Director General pursuant to section 235 of the School Education Act 1999 and consisting of the following classes:

- School administrators (principals and those as listed in regulation 127 of the School Education Regulations 2000);
- Teachers other than school administrators;
- Any other class as prescribed in regulation 127A of the School Education Regulations 2000.
- Education assistants' (government) general agreement 2016
- Public Service and Government Officers General Agreement 2014

### **Site managers**

Officers, including Principals, Line Managers and Residential College Managers, who have responsibility for overall management of any Department site.

### **Third party service providers of online applications**

Third Party Service Providers of online applications are any organisations, consultants, or independent contractors who render an online service or product to the Department/ Schools.

## 5. Related documents

### Relevant legislation or authority

*Censorship Act 1996 (WA)*

*Copyright Act 1968*

*Criminal Code Act Compilation Act 1913 (WA)*

*Cybercrime Act 2001(Cth)*

*Equal Opportunity Act 1984 (WA)*

*Freedom of Information Act 1992 (WA)*

*Privacy Act 1988 (Cth)*

*School Education Act 1999 (WA)*

*School Education Regulations 2000 (WA)*

*Sex Discrimination Act 1984 (Cth)*

### 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](#)

[Risk and Business Continuity Management](#)

[Student Behaviour in Public Schools](#)

[Software Use](#)

[Telecommunications Use](#)

### **Other documents**

[Access interpreting services \(staff only\)](#)

[Access translation services \(staff only\)](#)

[Access resources for online safety \(staff only\)](#)

[eSafety Commissioner](#)

[Escalate inappropriate social media content \(staff only\)](#)

[Manage online third party services at your school \(staff only\)](#)

[Report sexually explicit or child exploitation material \(staff only\)](#)

[Respond to a student disclosure of abuse \(staff only\)](#)

[Use copyright materials in schools \(staff only\)](#)

[Use of social media in your school \(staff only\)](#)

## 6. Contact information

### Policy manager:

Manager, Capability Support

### Policy contact officer:

Principal Project Officer, Capability Support

Telephone: (08) 9264 5309

Email: [E-Schooling@education.wa.edu.au](mailto:E-Schooling@education.wa.edu.au)

### Other:

ICT Customer Services Centre

Telephone: (08) 9264 5555 (metro)

Telephone: 1800 012 828 (regional)

Email: [customer.service.centre@education.wa.edu.au](mailto:customer.service.centre@education.wa.edu.au)

## 7. History of changes

<b>Effective date</b>	19 March 2019
<b>Last update date</b> <b>Procedure version no.</b>	3.0
<b>Notes</b>	The Students Online in Public Schools Policy has undergone a major review. This is the first set of procedures that supports the policy v3.0. There is no version 1.0 or 2.0 of the procedures. Endorsed by the Director General at Corporate Executive on 20 February 2019.

<b>Effective date</b>	19 March 2019
<b>Last update date</b>	10 April 2019
<b>Procedure version no.</b>	3.1
<b>Notes</b>	Minor changes to update a link in the guidance section of 3.4 as per D19/0156908.
<b>Effective date</b>	19 March 2019
<b>Last update date</b>	10 December 2019
<b>Procedure version no.</b>	3.2
<b>Notes</b>	Minor changes to s3.4 guidance and appendices G, H and I as per D19/0565452
<b>Effective date</b>	19 March 2019
<b>Last update date</b>	14 October 2022
<b>Procedure version no.</b>	3.3
<b>Notes</b>	Minor update to Contact details – D22/0762304
<b>Effective date</b>	19 March 2019
<b>Last update date</b>	16 December 2022
<b>Procedure version no.</b>	3.4
<b>Notes</b>	Minor changes to s3.3.1, s3.3.2, s3.5 guidance and definitions. Minor update to Contact Details. D22/0921560
<b>Effective date</b>	19 March 2019
<b>Last update date</b>	3 March 2023
<b>Procedure version no.</b>	3.5
<b>Notes</b>	Minor changes to s3.4 guidance and appendices G, H and I replaced. D23/0465888

## 8. Appendices

Appendix A: [Appendix A - Sample letter to parents](#) (DOCX file - 16.8kB)

Appendix B: [Appendix B - Permission for student to have an online service account](#) (DOCX file - 15.3kB)

Appendix C: [Appendix C - Online services acceptable use agreement \( K-Year2\)](#) (DOCX file - 15.3kB)

Appendix D: [Appendix D - Online services acceptable use agreement \(Years 3-6\)](#) (DOCX file - 15.5kB)

Appendix E: [Appendix E - Online services acceptable use agreement \(Years 7-12\)](#) (DOCX file - 16.2kB)

Appendix F: [Appendix F - Permission to publish students images and work for school purposes](#) (DOCX file - 15.7kB)

Appendix G: [Appendix G - Online Third-Party Services - Parent Letter](#) (DOCX file - 46.8kB)

Appendix H: [Appendix H - Online Third-Party Services - Parent Notification](#) (DOCX file - 48.8kB)

Appendix I: [Appendix I - Online Third-Party Services - Parent Consent and Agreement Form](#) (DOCX file - 59.6kB)

## 9. More information

### Supporting content

#### Policy

[Students Online in Public Schools Policy](#)

#### Procedure review date

19 March 2022

#### Procedure last updated

3 March 2023

---