GOVERNMENT OF
WESTERN AUSTRALIA

Department of
Education

Online Services Acceptable Use procedures

Effective date: 29 July 2025

Version: 1.2

Last update date: 5 August 2025

These procedures must be read in conjunction with the Online Services Acceptable Use policy.

Table of contents

These procedures must be read in conjunction with the Online Services Acceptable Use policy.

1. Policy supported

Online Services Acceptable Use policy

2. Scope

These procedures apply to all employees.

Guidance

These procedures apply to:

- accessing Department online services
- accessing any online service using Department owned devices.

3. Procedures

3.1 Informed view of risks and benefits

Line managers and principals must:

- refer to available guidance when reviewing the risks and benefits of online services
- support staff, students, and the school community in understanding the risks of online activities.

Guidance

Line managers and principals may share relevant information from the Department's intranet and discuss online safety procedures as part of professional development programs to promote proactive online safety education at all levels.

The Department provides access to online services and connectivity to corporate and external online services to enable access to information, communication and collaboration resources.

By accessing any Department online service or by using a Department owned device, employees give full agreement and commitment to comply with all relevant policies and give consent to logging, monitoring, auditing and disclosure of all use of these services.

Inappropriate use of Department online services or Department owned devices will be managed in accordance with relevant Department policies and procedures.

Disciplinary action for inappropriate use of Department online services may include suspension of access to online services, dismissal or termination of contract.

Line managers and principals should assign responsibility for staff development regarding these issues to an officer within the workplace. A range of associated cyber security training videos is available to staff via Online Professional Learning – check Ikon for details (staff only).

Line managers and principals should consider the risks with using social media and artificial intelligence, see Ikon for further information:

- Manage social media and electronic communication use (staff only)
- Use generative artificial intelligence technologies (staff only)

The TikTok application is not permitted on government devices (for example, phones, tablets or computers), as outlined in Cyber Security Notice 20230413007 – Restrictions on the use of the TikTok application on government issued devices, published by the Public Sector Commission via the CEO Gateway in April 2023. This aligns with advice from the Australian Government that the installation of the TikTok application on government devices poses a significant protective security risk and that government entities should prevent installation and remove existing instances of the application unless a legitimate business reason exists.

While the restriction on the use of the TikTok application does not apply to personal devices, employees who use personal devices to access Official and Official Sensitive data should carry out a formal risk assessment.

3.1.1 Personal information, privacy and confidentiality

Employees must:

- not share account username or password credentials
- treat all Department information, especially staff and student details, with the appropriate levels of sensitivity, privacy and confidentiality
- not establish a facility to automatically forward Department email to email addresses external to the Department's network
- not deliberately use any software services or products for the purpose of masking or obfuscating online activity.

Guidance

Line managers and principals should advise staff, students, and the school community, as needed, of appropriate standards of online behaviour and the risks associated with online activities.

Principals may refer to recommendations contained in the eSafety Commissioner's Best Practice Framework for Online Safety Education regarding proactive approaches to developing and implementing online safety education to every student, at every year level, and every stage.

Line Managers can refer staff to information available on the Department's intranet, relevant professional learning, and other government resources. For example, line managers may wish to discuss these procedures as part of staff professional development programs.

Employees should:

- think before posting a message, once posted it can be difficult, if not impossible, to remove
- not post comments or images that may be interpreted as being inappropriate, embarrassing or hurtful
- respect other people's content that is posted or shared. For example, a photo taken by a friend is their property, and should only be used with permission.

The Australian Government provides further information on the importance of online anonymity and protective online behaviours on the Office of the Children's eSafety Commissioner website .

3.2 Images and information

Line managers and principals must advise staff of the possible negative consequences of publishing identifying information on the Internet including images of themselves, other staff and students.

Employees must:

- confirm that any material planned for publication has the required approvals and has appropriate copyright and privacy clearance (refer to the Intellectual Property Policy and Copyright for Schools Guidelines)
- where possible, use a school owned device for taking student photographs, rather than personal cameras, phones or other internet connected devices.

Employees using personal cameras, phones, or other devices must:

- ensure that the settings prevent access to the photo library to safeguard student images
- transfer photographs to a school-owned device as soon as practicable and delete the images from their personal device.

Store photographs in line with the Department's Records Management policy and procedures.

3.2.1 Email and file sharing

Employees must:

- manage their email mailbox in accordance with Department Records Management Policy and Procedures
- use Department email and file sharing services for work-related purposes only
- carefully consider the need before sending bulk email messages to other staff members or distribution lists. Where necessary, consult with your principal (if at schools), the regional director (if at a Regional Office) or a director (if at Central Office) to obtain the appropriate approval
- comply with copyright and intellectual property requirements before posting, sharing, or storing any materials online.

3.3 Access to online devices and services

Line managers and principals must:

- only provide access to Department owned computer and communication devices when there is a demonstrated need and benefit to the Department
- remind staff to use all Department owned online devices and services in accordance with the Department's Code of Conduct and Standards (staff only)
- instruct staff to use all Department online services in accordance with the Department's Code of Conduct and Standards (staff only)
- manage inappropriate use of Department online services, and Department owned computer and communication devices in accordance with the relevant Department policy and procedure.

Employees must:

- use Department online services, and Department owned computer and communication devices in accordance with the Department's Code of Conduct and Standards (staff only)
- use Department online devices and services for work-related purposes only
- report lost mobile devices to the employee's principal or line manager and to the ICT Customer Service Centre at the earliest opportunity

- report online services that are no longer required to the ICT Customer Service Centre at the earliest opportunity.

Guidance

All mobile devices provided by the Department should be assigned to an individual. Shared services and devices are the responsibility of the principal or line manager, and a local use register should be maintained.

Line managers and principals can access mobile use reports available in SharePoint folders as an aid to managing the responsible use of mobile services.

Information about insurance for mobile devices is available on Ikon at Find information about insurance (staff only).

3.4 Security of online services

All employees must report to a principal or line manager, or directly to the ICT Customer Service Centre, any evidence or suspected compromise, incident or event that may have an impact on the security or effective operation of Department online services.

4. Definitions

Inappropriate content

Content considered unacceptable, unsuitable or harmful to students, staff or the school community, or that risks bringing the Department into disrepute. Such content includes but is not limited to material that is pornographic, racist, sexist, inflammatory, threatening, bullying, hateful, obscene or abusive in nature or content which promotes or encourages inappropriate, violent, or illegal activities.

Online services

Any online service or system that may be accessed from Department owned devices, personally owned devices or via other external connectivity, through digital or telecommunication networks or licences provided by the Department, including but not limited to:

- telecommunication (fixed and mobile) and related services
- email, calendaring, instant messaging, web conferencing and discussion groups
- content management systems, file sharing and storage
- internet and intranet access, Web browsing and social media.

5. Related documents

Relevant legislation or authority

Children and Community Services Act 2004

Commissioner's Instruction 40 Ethical Foundations

Copyright Amendment (Digital Agenda) Act 2000

Public Sector Management Act 1994

Related Department policies

Cyber Security

Duty of Care for Public School Students

Intellectual Property

Risk and Business Continuity Management

Software Use

Staff Conduct and Discipline

Student Mobile Phones in Public Schools

Students Online in Public Schools

Other documents

Access software licences (staff only)

Code of Conduct and Standards (staff only)

Copyright for Schools Guidelines

Manage your password and user validation question (staff only)

Manage users on shared devices in schools (staff only)

Protect student and network security in schools (staff only)

Use copyright materials in schools (staff only)

Use social media in your school (staff only)

6. Contact information

Policy manager:

Director, Operations and Customer Service, ICT Directorate

Policy contact officer:

Principal Consultant, ICT Directorate

Other contact:

Customer Service Centre (CSC)

T: (08) 9264 5555

7:30 am – 5:00 pm Monday to Friday (excluding public holidays)

7. History of changes

Effective date	29 July 2025
Last update date **Procedure version no.**	1.0
Notes	Director General approved for publication on 18 June 2025.

Effective date	29 July 2025
Last update date	29 July 2025
Procedure version no.	1.1
Notes	Minor changes to links and removal of Social Media in Schools document (Approval D25/0632836)

Effective date	29 July 2025
Last update date	5 August 2025
Procedure version no.	1.2
Notes	Minor changes to links 'Intellectual Property policy' and 'Records Management policy and procedures'. Renamed link 'Commissioner's Instruction 40: Ethical Foundations' (Approval D25/0662263).

8. More information

Supporting content

Policy

Online Services Acceptable Use policy

Procedure review date

29 July 2028

Procedure last updated

5 August 2025