GOVERNMENT OF
WESTERN AUSTRALIA

Department of
Education

Cyber Security Policy

Effective date: 9 August 2022

Version: 3.1

Last update date: 17 November 2022

Table of contents

1. Policy statement **3**

2. Policy rules **4**

3. Responsibility for Implementation and Compliance **5**

4. Scope **5**

5. Supporting Procedures **5**

6. Definitions **5**

7. Related documents **6**

8. Contact information **8**

9. History of changes **9**

10. More information **10**

Policy review date 10

Policy last updated 10

1. Policy statement

The Department of Education (the Department) implements measures to protect the Department's electronic information, infrastructure and services from theft, unauthorised access or use, disclosure, modification or destruction during the information lifecycle.

2. Policy rules

Employees must:

- only use the Department's Information and Communication Technologies (ICT) resources to which they have been granted access privileges;
- prevent unauthorised disclosure of data;
- prevent unauthorised access to information on an inactive workstation;
- report any suspicion of, or known, security threats or breaches to their line manager or the ICT Customer Service Centre; and
- only use the Department's ICT resources for:
  - work/business and educational purposes; or
  - personal use when it is not for commercial gain or in any way counterproductive to the business of the Department (refer to Telecommunications Use Policy).

Principals must maintain ICT infrastructure security in schools.

Site managers must:

- confirm that employees are made aware of the requirements of this policy; and
- endorse the use of the Department ICT infrastructure by non- employees and confirm supervision by a Department employee.

Guidance

Employees are accountable for all actions and functions performed on their account.

Employees are encouraged to use private email services for conducting personal business rather than Department provided email facilities. There is no expectation of privacy when using Department email for private use.

3. Responsibility for Implementation and Compliance

Principals and line managers are responsible for implementing the policy.

Line managers are responsible for compliance monitoring.

4. Scope

This policy applies to all Department employees.

5. Supporting Procedures

Cyber Security Procedures

6. Definitions

Administrator Account

An administrator account is a user account with high-level privileges to make changes on a computer that will affect other users of the computer. Administrators can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.

DAM

Department of Education Account Manager (DAM) administrators use the DAM tool to give schools, business areas, employees and visitors access to online services in accordance with their employment position or agreed contract access requirements.

Department Employee

A Department employee is any person paid by the Department to provide a service, be it full time or part time as a staff member or teacher, or as a contractor for a short time or long time.

Department ICT Infrastructure

All physical, virtual and cloud-based infrastructure and software owned by the Department, including physical or logical connection to the network, including use of Corporate Information Systems.

Generic Account

An account created which cannot be directly attributed to an identifiable, auditable user. For example, admin front desk, admin temp, temp technician and temp teacher.

Non-employee

A volunteer or a work-place experience person, or other non-paid individual using the Department ICT infrastructure, is not an employee. For the purposes of this policy, they are classified as non-employees.

Service Account

A service account is a user account that is created explicitly to provide a security context for services running on Windows Server operating systems. The security context determines the service's ability to access local and network resources. The Windows operating systems rely on services to run various features.

Site Manager

Officers, including principals, site managers and line managers, who have executive responsibility for overall management and control of any Department workplace.

7. Related documents

Relevant legislation or authority

Copyright Act 1968

Criminal Code Act Compilation Act 1913 (WA)(CI)

Privacy Act 1988

Government of Western Australia's Cyber Security Policy

School Education Act 1999

Related Department policies

Staff Conduct and Discipline

Records Management

Risk and Business Continuity Management

Telecommunications Use

School Security for Public Schools

Other documents

Corruption Prevention and Detection

Encryption of Removable Media Guidelines (staff only)

Manage records at your school (staff only)

8. Contact information

Policy manager:

Director, ICT Operations and Customer Service

Policy contact officer:

Cyber Security Consultant

Other contact:

Customer Service Centre (CSC)

T: (08) 9264 5555

7.30am – 5.00pm Monday to Friday (excluding public holidays)

9. History of changes

Effective date	18 August 2015
Last update date **Policy version no.**	2.0
Notes	Major review undertaken and split into policy and procedures. Endorsed by Corporate Executive 14 November 2014.

Effective date	18 August 2015
Last update date **Policy version no.**	2.1
Notes	Corrected typing error D15/0324518 Version 2.1 updated prior to version 2.0 becoming effective.

Effective date	9 August 2022
Last update date **Policy version no.**	3.0
Notes	The new Cyber Security Policy and Procedures, replaces the Information and Communication Technologies Security policy and procedures. Approved by the Director General on 14 July 2022 D22/0539066. Summary of changes to the Cyber Security Policy on Ikon (staff only).

Effective date	9 August 2022
Last update date	17 November 2022
Policy version no.	3.1
Notes	Minor change to update links D22/0841360

10. More information

Supporting content

Procedure

Cyber Security Procedures

Policy review date

9 August 2025

Policy last updated

17 November 2022