GOVERNMENT OF
WESTERN AUSTRALIA

Department of
Education

Information and Communication Technologies Security Policy

Effective date: 18 August 2015

Version: 2.1

Accurate at the time of printing 29/07/2021.

Table of contents

1. Policy statement

The Department of Education (the Department) implements measures to protect the Department's computerised information, computer 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 technology (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 Customer Service Centre; and
- only use the Department's ICT resources;
    - for work/business and educational purposes; or
    - for personal use provided it is not for commercial gain or in any way counterproductive to the business of the Department.

In addition, principals must maintain infrastructure security in schools.

Guidance

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

3. Responsibility for Implementation and Compliance

Principals and line managers are responsible for implementation of the policy.

The Chief Information Officer is responsible for compliance monitoring.

4. Scope

This policy applies to all Department employees.

5. Supporting Procedures

Information and Communication Technologies Security Procedures

6. Definitions

Department ICT infrastructure

All physical equipment and software owned by the Department, including physical or logical connection to the network and/or 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.

7. Related documents

Relevant legislation or authority

Copyright Act 1968

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

Privacy Act 1988

Public Sector Commissioner's Circular 2010-05 – Computer Information and Internet Security

School Education Act 1999

Related Department policies

Corruption Prevention and Detection

Staff Conduct and Discipline

Records Management

Risk and Business Continuity Management

Telecommunications Use

School Security for Public Schools

Other documents

Encryption of Removable Media Guidelines (staff only)

Records Management Manual for School and Campus Records (staff only)

8. Contact information

Policy manager:

Director, ICT Infrastructure and Telecommunications

Policy contact officer:

ICT Security Administrator

T: (08) 9264 5114

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.

10. More information

Supporting content

Procedure

Information and Communication Technologies Security Procedures

Policy review date

18 August 2018