Department of
Education

Information and Communication Technologies Security Procedures

Effective date: 18 August 2015

Version: 2.1

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

These procedures must be read in conjunction with the Information and Communication Technologies Security Policy.

Table of contents

These procedures must be read in conjunction with the Information and Communication Technologies Security Policy.

1. Policy supported

Information and Communication Technologies Security Policy

2. Scope

These procedures apply to all employees.

3. Procedures

3.1 Passwords and user identification

Employees must not disclose their password or allow another person to access the Department of Education's (the Department's) information and communication technology (ICT) infrastructure using their user identification number (user ID).

Employees responsible for password and user ID management must:

- where technically feasible, use the system password setting standards detailed in Appendix A;
- create a separate user ID for every person requiring access to the Department's infrastructure and not create generic accounts; and
- not establish permissions to enable access to one user's account from another.

Line managers must confirm that at all times, any individual user of any section of the Department's ICT infrastructure, is identifiable and auditable.

Guidance

A unique user ID is created for every individual user of the Department's ICT infrastructure. This is a significant factor in protecting staff and student users, the Department systems, and the information stored on both the local and central networks from malicious or inappropriate access and misuse.

3.2 Portable storage device security

Employees must:

- adhere to the Encryption of Removable Media Guidelines (staff only) when using any form of communication, computing or portable storage device to store any confidential or sensitive information belonging to the Department;
- mitigate the risk of introducing malware into the Department's ICT infrastructure; and
- prior to the disposal of any and all forms of ICT equipment capable of storing sensitive or confidential information belonging to the Department, securely delete that information in accordance with Department guidelines found at the ICT Equipment Disposal (staff only) web page.

Guidance

Examples of equipment capable of storing sensitive or confidential information include but is not limited to USB thumb drives, external hard drives, laptops, iPads, PDAs, mobile phones, printers, scanners, photo copiers, multifunction devices.

3.3 Work station screen lockout

If it has not been automatically set, employees must set a 10 minute lock out on their workstation.

Guidance

An automatic screen lockout time of 10 minutes is globally set across the Department's ICT infrastructure on centrally managed devices.

Employees have a responsibility to prevent unauthorised access to information on their workstation. To facilitate this employees should screen lock their computer if leaving their desk for more than five minutes.

3.4 Access for external parties

Line managers must:

- use the approved mechanism for providing external parties temporary access to the Department's ICT infrastructure; and
- advise external parties that their access to the Department's ICT infrastructure is subject to their adherence to the Information Communication Technologies Security Policy and Procedures.

Guidance

External parties include temporary/relief/visiting staff or members of the public, for example, assisting parents, medical staff and contractors.

3.5 Infrastructure security in schools

Principals will maintain infrastructure security in schools and implement effective information security practices.

Guidance

The following measures should be in place for infrastructure security in schools:

- confirm correct security setting;
- implement effective exit procedures;
- carefully manage security groups;
- review the location of sensitive information;
- keep network operating systems up-to-date;
- deploy up-to-date anti-virus software;
- understand application system security requirements; and
- secure equipment.

See Appendix B: Infrastructure Security for Schools Guidelines for further information.

4. 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.

5. 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)

6. Contact information

Policy manager:

Director, ICT Infrastructure and Telecommunications

Policy contact officer:

ICT Security Administrator

T: (08) 9264 5114

Other:

Customer Service Centre (CSC)

T: (08) 9264 5555

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

7. History of changes

Effective date	18 August 2015
Last update date	
Policy version no.	
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.	
Notes	Updated inconsistencies in Appendix A D15/0324895. Version 2.1 updated prior to version 2.0 becoming effective.

8. Appendices

Appendix A: System password standard settings (PDF file - 43.3kB)

Appendix B: Infrastructure security for schools guidelines (PDF file - 70.5kB)

9. More information

Supporting content

Policy

Information and Communication Technologies Security Policy

Procedure review date

18 August 2018