



Department of
Education

INFORMATION BREACH POLICY

INFORMATION BREACH PROCEDURES

This PDF contains the following documents

Document 1:

Information Breach Policy v1.0

Effective: 12 November 2024

Document 2:

Information Breach Procedures v1.0

Effective: 12 November 2024



Department of
Education

INFORMATION BREACH POLICY

EFFECTIVE: 12 NOVEMBER 2024

VERSION: 1.0 FINAL

1. Policy statement

The Department of Education (the Department) is committed to preventing information breaches and implements measures to safeguard the data and information it collects, holds, manages, uses, and discloses as part of its functions and activities outlined in the *Privacy and Responsible Information Sharing Bill 2024*, *School Education Act 1999*, or any other written law.

2. Policy rules

This Policy is a mandatory requirement under the Privacy and Responsible Information Sharing (PRIS) Policy and Framework.

All employees must:

- only access and use official and confidential information for authorised purposes.
- ensure the appropriate roles and responsibilities are defined in the processes and procedures to address the circumstances of an information breach.
- comply with the Information Breach Procedures.

Guidance

See the Department's *Code of Conduct* for further information on professional use of information.

This policy is a mandatory requirement under the Privacy and Responsible Information Sharing (PRIS) Policy and Framework.

Information Privacy and Data Governance team may request compliance audits to assess the level of adherence to the policy and provide updates to the Director General, Managers, Information Stewards, Principals, and other relevant individuals regarding the findings of compliance monitoring activities.

3. Responsibility for implementation and compliance

All employees are responsible for implementing this policy.

The Information Privacy and Data Governance team is responsible for compliance monitoring.

4. Scope

This policy applies to all employees.

5. Supporting procedures

Information Breach Procedures

6. Definitions

Information

Means information, records or data that has been processed in a way as to be meaningful to the person who receives it. The term 'data' and 'information' can be used interchangeably and should be taken to mean both data and information in this document.

Information Breach

Occurs when there is unauthorised access, disclosure or loss of information and may be caused by malicious action, human error, or a failure of handling or systems.

7. Related documents

Relevant legislation or authority

[Australian Government Protective Security Policy Framework](#)

[Children and Community Services Act 2004](#)

[Corruption Crime and Misconduct Act 2003 \(WA\)](#)

[Criminal Code Act Compilation Act 1913 \(WA\)](#)

[Criminal Procedures Act 2004 \(WA\)](#)

[Equal Opportunity Act 1984 \(WA\)](#)

[Evidence Act 1906 \(WA\)](#)

[Freedom of Information Act 1992 \(WA\)](#)

[Freedom of Information Regulations 1993 \(WA\)](#)

[Parliamentary Commissioner Act 1971](#)

[Privacy Act 1988 \(Cwlth\)](#)

[Privacy and Responsible Information Sharing Bill 2024 \(WA\)](#)

[Public Interest Disclosure Act \(2003\) \(WA\)](#)

[Public Sector Management Act 1994 \(WA\)](#)

[School Education Act 1999 \(WA\)](#)

[School Education Regulations 2000 \(WA\)](#)

[School Education \(Student Residential Colleges\) Regulations 2017\)](#)

[Schools Curriculum and Standards Authority Act 1997 \(WA\)](#)

[State Records Act 2000 \(WA\)](#)

[Teacher Registration Act 2012 \(WA\)](#)

[Teacher Registration \(General\) Regulations 2012](#)

Related Department policies

[Child Protection in Department of Education Sites](#)

[Councils and Boards in Public Schools](#)

[Code of Conduct](#)

[Complaints and Notification](#)

[Criminal History Screening for Department of Education Sites](#)

[Cyber Security](#)

[Duty of Care for Public School Students](#)

[Employee Performance](#)

[Enrolment in Public Schools](#)

[Injury Management and Workers' Compensation](#) (staff personal information)

[Integrity Framework](#)

[Managing a Breach of the Public Sector Standard Claims](#) (staff/student personal information)

[Records Management](#)

[Recruitment, Selection and Appointment](#)

[Research Conducted on Department of Education Sites by External Parties](#)

[Risk and Business Continuity](#)

[Security for Public Schools and Residential Facilities](#)

[Software Use](#)

[Staff Conduct and Discipline](#)

[Student Attendance in Public Schools](#)

[Student Health in Public Schools](#)

[Students Online in Public Schools](#)

[Telecommunications Use](#)

[Working with Children Checks in Department of Education Sites](#)

Other documents

Delegation information relating to the disclosure of information

Information Breach Procedures

[Manage student files at your school \(staff only\)](#)

[Manage student information in SIS Classic \(staff only\)](#)

[Western Australian Government Cyber Security Policy](#)

[Western Australian Information Classification Policy](#)

[Western Australian Whole of Government Open Data Policy](#)

8. Contact information

Policy manager: Director Business and Customer Services

Policy contact officer: Principal Consultant Information and Data Governance

E: businessandcustomerservices.infoprivacygovernance@education.wa.edu.au

9. Review date

12 November 2027

10. History of changes

Effective date	Last update date	Policy version no.	Ref no.	Notes
This table will be completed by the Governance Unit.				
12 November 2024		1.0	D24/0491921	New policy, endorsed by the Director General at the Corporate Executive meeting held on 11 September 2024. D24/0653243



Department of
Education

INFORMATION BREACH PROCEDURES

EFFECTIVE: 12 NOVEMBER 2024

VERSION: 1.0 FINAL

CONTENTS

1	POLICY SUPPORTED.....	3
2	SCOPE	3
3	PROCEDURES.....	3
	3.1 CONTAIN THE INFORMATION BREACH.....	3
	3.2 ASSESS THE DETAILS OF THE INFORMATION BREACH	3
	3.3 NOTIFY THE RELEVANT AUTHORITIES	4
4	DEFINITIONS	5
5	RELATED DOCUMENTS	6
6	CONTACT INFORMATION.....	8
7	REVIEW DATE	8
8	HISTORY OF CHANGES	9

1 POLICY SUPPORTED

Information Breach Policy

2 SCOPE

These procedures apply to all employees.

3 PROCEDURES

3.1 CONTAIN THE INFORMATION BREACH

The employee who discovers a breach must:

- take steps to contain the breach by limiting distribution of the affected information and preventing further compromise.
- immediately inform their principal/line manager.

The principal/line manager must:

- confirm that steps have been taken to contain the breach.
- document details of the steps taken to aid in the assessment, review, and developing of preventative actions and/or education programs and training material.
- seek advice from the Departments Standards and Integrity Directorate in cases of potential breaches of discipline or conduct.
- inform the Information Custodian.
- if required, escalate the incident to the Information Privacy and Governance Team for them to carry out further investigations and reporting.

The Information Custodian must:

- have an oversight of the breach related to their information asset to review and continually update risk mitigation strategies

The Information Privacy and Governance Team must:

- support the communications related to breaches.
- determine if other escalation or notification is required.

3.2 ASSESS THE DETAILS OF THE INFORMATION BREACH

The principal/line manager must:

- carry out an initial and impartial assessment depending on the breach circumstances.

For escalated breaches, the Information Privacy and Governance Team must:

- seek advice from the Departments Standards and Integrity Directorate in cases of potential breaches of discipline or misconduct.

Guidance:

Factors to consider when assessing an information breach:

Details of the breach: Assessors should evaluate the type and sensitivity of breached information, identify affected individuals, and determine the extent and impact of the breach.

Source of the breach: Assessors must investigate the source of the breach to identify the root cause and contributing factors, determining if it was due to malicious intent, human error, or negligence. They should understand the circumstances leading to the breach, assess if it was a system failure or a procedural issue, and determine if it was an isolated incident or an ongoing risk.

Impact assessment: Assessors must evaluate the nature of the breach, affected individuals, and the type of compromised information. They should determine the extent of the breach and assess potential current and future harm to both the affected individuals and the Department.

Extent: Assessors must quantify the amount of data or number of records breached, the duration the breach went undetected, and whether the information has been recovered.

Harm to individuals and the Department: Potential harm to individuals includes identity theft, threats to personal safety, damage to reputation, loss of business opportunities, and financial loss. For the Department, the breach could impact service capacity, result in loss of reputation and public trust, financial loss, exposure of sensitive information, loss of assets, and risk of regulatory penalties or legal liability.

3.3 NOTIFY THE RELEVANT AUTHORITIES

The principal/line manager must inform:

- the Information Privacy and Governance Team.
- other responsible officers in accordance with Western Australian Information Classification Policy.
- the Standards and Integrity Directorate if the breach constitutes a breach of discipline or contravention of the Code of Conduct.

The Information Privacy and Governance Team must:

- provide advice on the management of a breach.
- maintain the information breach register and ensure it is stored and managed on the Electronic Document Records Management System (TRIM).
- conduct an annual review of information breaches to determine the inclusion in the Annual Report.
- review and make recommendations to implement measures and prevent future breaches.

- notify and report the breach to the Information Commissioner if the breach meets the requirements of the Notifiable Information Breach Scheme under the Privacy and Responsible Information Breach Bill 2024.
- review the process and the breach event to ensure all notification have been finalised to determine if further action is required.
- implement and review the Information Breach Policy and supporting documents.
- develop education programs and training materials.

4 DEFINITIONS

Aboriginal Information

Aboriginal Information refers to information, including family history that relates to Aboriginal people and their ancestors.

Discriminatory Harm

Discriminatory Harm refers to information that causes a person to be treated differently due to ethnicity, gender, disability, age, religious belief, pregnancy, or sexual orientation (for example, details of religious beliefs that leads to public persecution).

Financial Harm

Financial harm refers to financial loss or being unable to access one's money (for example, when a third-party gains access to bank account).

Health Information

Health information refers to personal or sensitive information or an opinion about an identified or reasonably identifiable individual's health, illness, disability or injury. Including an individual's expressed wishes about the future provision of health services, or a health service provided or to be provided to an individual. Health information also includes other personal information collected, to provide or in providing a health service to an individual. Health information is regulated in Western Australia under the Health Services Act 2016.

Information Privacy Principle (IPP) Entity

IPP entity refers to a Minister, Parliamentary Secretary, a public entity or contracted service provider thereby, the Department of Education is referred to as an IPP entity for the purposes of this document.

Notifiable Information Breach

A notifiable information breach occurs when personal information held by an IPP entity is accessed, disclosed, or lost without authorisation and if a reasonable person would conclude that this access or disclosure is likely to result in serious harm to the affected individual. Serious harm refers to discriminatory, financial, physical, psychological or emotional, or reputational harm).

Personal Information

Personal Information including sensitive information, means information or an opinion about an identified or reasonably identifiable individual, living or dead, whether true or not, and can be recorded in a material form or not.

Physical Harm

Physical harm refers to risk of physical harm or intimidation (for example, disclosure of a physical address to someone who wishes to cause physical harm to another).

Psychological or Emotional Harm

Psychological or emotional harm including cultural harm, means having personal information available that causes anxiety, embarrassment, depression or hurt feelings (for example, potential availability of personal details or family circumstances, gender, ethnicity, or health information).

Reputational Harm

Reputational harm is damage to an individual or an IPP entity within the community or negative publicity that damages a reputation (for example, disclosure of information that negatively impacts an image).

Threats of harm

Threat of harm arises from the availability of personal information from an information (or data) breach (for example, threats of blackmail or extortion).

5 RELATED DOCUMENTS

Relevant legislation or authority

[Australian Government Protective Security Policy Framework](#)

[Children and Community Services Act 2004](#)

[Corruption Crime and Misconduct Act 2003 \(WA\)](#)

[Criminal Code Act Compilation Act 1913 \(WA\)](#)

[Criminal Procedures Act 2004 \(WA\)](#)

[Equal Opportunities Act 1984 \(WA\)](#)

[Evidence Act 1906 \(WA\)](#)

[Freedom of Information Act 1992 \(WA\)](#)

[Freedom of Information Regulations 1993 \(WA\)](#)

[Parliamentary Commissioner Act 1971](#)

[Privacy Act 1988 \(Cwlth\)](#)

[Privacy and Responsible Information Sharing Bill 2024 \(WA\)](#)

[Public Interest Disclosure Act \(2003\) \(WA\)](#)

[Public Sector Management Act 1994 \(WA\)](#)

[School Education Act 1999 \(WA\)](#)

[School Education Regulations 2000 \(WA\)](#)

[Schools Curriculum and Standards Authority Act 1997 \(WA\)](#)

[State Records Act 2000 \(WA\)](#)

[Teacher Registration Act 2012 \(WA\)](#)

[Teacher Registration \(General\) Regulations 2012](#)

Related Department policies

[Child Protection in Department of Education Sites](#)

[Councils and Boards in Public Schools](#)

[Code of Conduct](#)

[Complaints and Notification](#)

[Criminal History Screening for Department of Education Sites](#)

[Cyber Security](#)

[Duty of Care for Public School Students](#)

[Employee Performance](#)

[Enrolment in Public Schools](#)

[Injury Management and Workers' Compensation](#) (staff personal information)

[Integrity Framework](#)

[Managing a Breach of the Public Sector Standard Claims](#) (staff/student personal information)

[Records Management](#)

[Recruitment, Selection and Appointment](#)

[Research Conducted on Department of Education Sites by External Parties](#)

[Risk and Business Continuity](#)

[School Security for Public Schools and Residential Facilities](#)

Software Use

Staff Conduct and Discipline

Student Attendance in Public Schools

Student Health in Public Schools

Students Online in Public Schools

Telecommunications Use

Working with Children Checks in Department of Education Sites

Other documents

Delegation information relating to the disclosure of information

Manage student files at your school (staff only)

Manage student information in SIS Classic (staff only)

Western Australian Government Cyber Security Policy

Western Australian Information Classification Policy

Western Australian Whole of Government Open Data Policy

6 CONTACT INFORMATION

Policy manager:

Director, Business and Customer Services

Policy contact officer:

Principal Consultant, Information and Data Governance

E: businessandcustomerservices.infoprivacygovernance@education.wa.edu.au

7 REVIEW DATE

12 November 2027

8 HISTORY OF CHANGES

Effective date	Last update date	Policy version no.	Ref no.	Notes
This table will be completed by the Governance Unit.				
12 November 2024		1.0	D24/0551676	New procedures, endorsed by the Director General at the Corporate Executive meeting held on 11 September 2024. D24/0653243