GOVERNMENT OF WESTERN AUSTRALIA

DFES
Department of Fire & Emergency Services

Information Breach Statement

The Department of Fire and Emergency Services (DFES) handles information in support of community safety and operational activities. DFES is committed to protecting this information and responding appropriately to any suspected or actual information breach, including taking steps to minimise any harm to individuals and manage impacts to the agency.

This document outlines how DFES manages information breaches in accordance with:

- the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act)
- the WA Government Cyber Security Policy
- the WA Government Information Classification Policy
- the *State Records Act 2000*.

Information breach means unauthorised access to, unauthorised disclosure of, or loss of:

- personal information held by DFES, or
- information shared with or by DFES under an Information Sharing Agreement made under the PRIS Act.

For the purposes of this document, information includes any recorded or communicated material in any form, including electronic, paper-based, verbal, visual or recorded formats.

Information breaches can occur through the loss of any information due to human error, insider threats, malicious attacks, system failures or physical security incidents (e.g. theft).

DFES is committed to the security and integrity of its information and to manage the risk of potential information breaches by ensuring:

- Access to information is granted based on defined roles and responsibilities and on a need-to-know basis, so that DFES personnel can effectively carry out their duties.
- Information is only used as required to enable DFES to effectively perform its functions.
- Information is only shared or disclosed where authorised in accordance with DFES policies and applicable legislation.
- Information is stored in appropriate systems and managed accordingly, including secure deletion or disposal when no longer required, in accordance with applicable legislation or policy.
- Security updates are applied in a timely manner to DFES systems to reduce the risk of malicious activity.
- DFES devices are secured in accordance with organisational security requirements.
- Contracted third parties are bound by DFES information and secure policies and requirements, where appropriate.

Our commitments

If a suspected or actual information breach occurs, DFES will:

- **Contain:** Act quickly to stop further unauthorised access or disclosure and secure affected information.
- **Assess:** Undertake an initial assessment of the nature of the information involved and the potential impact of the information breach.
- **Investigate:** Establish the cause of the information breach, how it occurred and confirm what information was affected.
- **Mitigate:** Take appropriate steps to limit the impact of the information breach and reduce any ongoing risk to the security of the information.
- **Notify:** Inform the WA Information Commissioner, Chief Data Officer and affected individuals where required, and keep the community informed where appropriate.
- **Review:** Learn from the incident and strengthen our systems, processes training, and culture to reduce the risk of recurrence.

Accountability and transparency

- The DFES Privacy Officer is responsible for coordinating information breach management and notifications.
- A register of information breaches is maintained, and relevant statistics are reported in the DFES Annual Report, as required under the PRIS Act.
- This document is made publicly available.

Your role

If you believe your personal information has been involved in an information breach, or you become aware of a possible incident, please report it to DFES as soon as possible.

Contact us — Privacy Officer

Assistant Director, Information Services
privacy@dfes.wa.gov.au
GPO Box P1174
Perth WA 6844, Australia

Review

This document will be reviewed regularly to reflect changes in legislation, technology, and best practice.

Current as at: 01 July 2026 · Next review: 07 July 2028