



Office of the Victorian
Information Commissioner

Investigation into the data breach of student information held by the Department of Education

Investigation report – October 2026

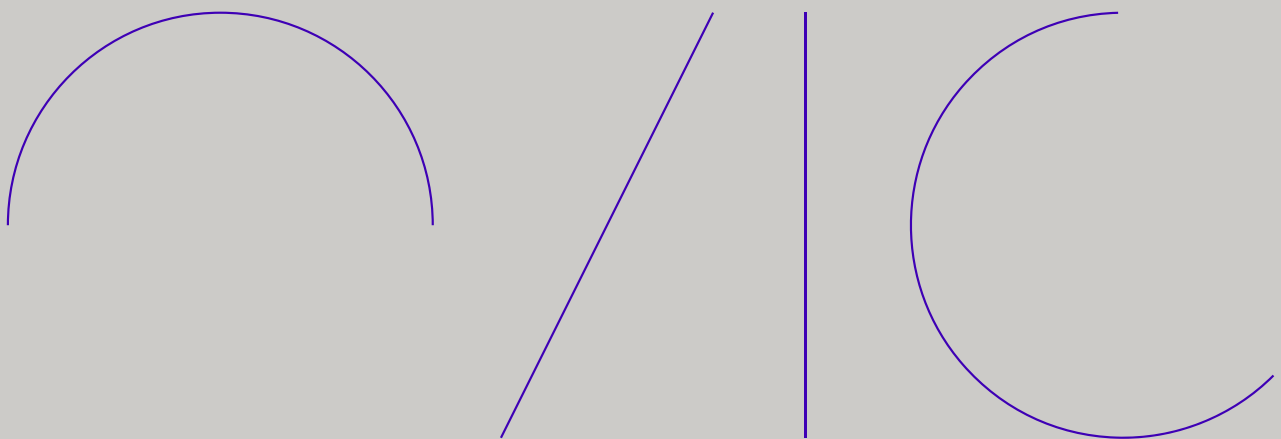


Table of Contents

Background	3
What happened	3
Why we investigated.....	3
What we investigated	4
Timeline of events	5
What we found	6
Issue 1: Non-compliance with the Department’s patching policy	6
Issue 2: Inadequate vulnerability management	7
Issue 3: Failure of the Information Security Policy Framework	8
Issue 4: Ineffective records management	8
What we concluded.....	9
Recommendations.....	9
Vulnerability detection and patching policies and procedures	9
Information security policy and practices for school operations	9
Records management policies and procedures	10
How the Department responded to the investigation	10
Appendix A – The Department’s response	11

Background

What happened

1. On 7 January 2026, the Department of Education (**the Department**) notified OVIC of a successful and highly sophisticated cyberattack on its systems.
2. The malicious attacker achieved this by compromising the Information Technology (IT) system of one of the Department's schools.
3. The information accessed and later found to have been taken, included every government school student's first name and surname, the school they attend, their year level, and school email addresses and encrypted passwords. The same details of hundreds of thousands of former students were also contained in the database and confirmed as affected by the data breach.

Why we investigated

4. Students and their families have a reasonable expectation that the Department protects the privacy and security of their personal information.
5. This expectation is reinforced by legally binding frameworks and strict accountability for how personal information is collected and managed.
6. All Victorian government schools must comply with Victorian privacy law and the Department's Schools' Privacy Policy which explains how Victorian government schools collect and manage personal information.
7. Compromise of the Department's systems had serious implications for students and families, with concerns about their location becoming known.
8. Such concerns are heightened for children and families experiencing or at risk of family violence, seeking asylum, subject to court orders protecting their safety or children living in foster or kinship care.
9. While there was no evidence provided to OVIC to indicate further misuse or disclosure of the information immediately after the cyberattack, it remains that a malicious attacker made a copy of that information and could misuse or disclose the information at some time in the future.

What we investigated

10. OVIC commenced the investigation in January 2026 using its powers set out in the *Privacy and Data Protection Act 2014 (PDP Act)*.¹
11. The objective of the investigation was to consider whether the Department contravened the Information Privacy Principles (IPPs)² and/or the Victorian Protective Data Security Standards (VPDSS).³
12. The *Guidelines to the Information Privacy Principles*⁴ explain how the IPPs should be interpreted and applied. They set the standard for how Victorian Public Sector organisations should manage personal information.
13. The investigation specifically considered:
 - whether the Department took reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure (IPP 4.1)
 - whether the Department took reasonable steps to destroy or permanently deidentify personal information if it is no longer needed for any purpose (IPP 4.2).
14. The VPDSS were considered to the extent that they are considered ‘reasonable steps’ for complying with the IPPs.
15. When determining whether a particular step is ‘reasonable’, organisations must consider the potential impact of a possible security breach of the information they hold. What is reasonable depends on the circumstances. The requirement to take reasonable steps supports a risk-based approach to the security of personal information.
16. In this case, the information was about children and young people and, by extension, their families. A data breach of this information could pose a threat to their safety or wellbeing, particularly where they have vulnerabilities such as those identified above. This means that IPP 4.1 requires the Department to implement measures proportionate to the potential privacy risks to students and their families and the potential harm caused to them.

¹ The investigation commenced under sections 8C(2)(e) and 8D(2)(b) of the PDP Act.

² The 10 IPPs are set out in Schedule 1 of the PDP Act. The IPPs are the core of privacy law in Victoria and set out the minimum standard for how Victorian public sector organisations should manage personal information.

³ The VPDSS establish 12 high level mandatory requirements to protect public sector information across all security areas including governance, information security, personnel security, Information Communications Technology (ICT) security and physical security.

⁴ OVIC website, <https://ovic.vic.gov.au/privacy/resources-for-organisations/guidelines-to-the-information-privacy-principles/>

Timeline of events

17. While the Department was unable to precisely identify when the data breach happened, a post-incident report found that the earliest evidence of malicious activity was on 6 November 2025, with high confidence that the exploitation occurred prior to this first observed date.

18. The following shows the timeline of key events associated with the cyberattack:

- 1** **27 October 2025, 10.00am**
Australian Signals Directorate released a critical alert
- 2** **27 October 2025, 10.01am**
Department of Government Services alerted the Department of Education
- 3** **27 October 2025, 4.32pm**
The Department of Education sent a directive to all school technicians
- 4** **On or before 6 November 2025**
The cyberattack occurred
- 5** **2 December 2025, around 5.30pm**
The Department of Education's vendor notified it of the detection of significant threats
- 6** **3 December 2025**
The Department of Education activated its Cyber Security Incident Response Plan
- 7** **3 December 2025**
The first Cyber Security Incident Response Team meeting occurred
- 8** **4 December 2025**
The Department of Education re-sent the advisory to school technicians
- 9** **5 December 2025 to 30 December 2025**
Forensic investigations of the incident were conducted and containment and remediation actions were taken
- 10** **23 December 2025**
Forensic analysis identified that data had been exfiltrated
- 11** **24 December 2025**
The Department of Education's Incident Management Team met for the first time
- 12** **14 January 2026**
The media commenced reporting on the cyberattack

What we found

Issue 1: Non-compliance with the Department's patching policy

19. The Department has policies and procedures that aim to ensure the timely, secure and auditable patching (software updates) of IT systems across the Department and its schools.
20. The Department's IT Network Security Standard requires that 'all departmental owned and maintained networks and electronic communications devices will be updated with the latest but stable patches released by the respective vendors. Additionally, schools are required to implement the controls outlined in the Department's Information Security Policy.
21. According to the Information Security Policy, regular software updates are essential to maintain the security of devices and applications:

It is crucial that schools ensure their IT support technicians regularly perform risk-prioritised patching or vulnerability management for all systems, infrastructure and software applications under the school's responsibility.

The Technical Support to Schools Program provides specialist technicians to deliver on-site scheduled support for schools, which can assist in this process. Refer to Technologies and ICT Services Policy.

22. In the cyberattack being investigated, timely and effective patching did not occur at the school level.
23. Upon receiving a critical security advisory from the Department of Government Services on 27 October 2025, the Department issued a directive to the Technical Support for Schools Program (TSSP)⁵ seeking assistance to inform schools of the vulnerability and risk of exploitation. The TSSP notified schools of the vulnerability and steps to remediate (patch) relevant servers on the same day. However, not all schools followed the advice.
24. The Department's governance of the TSSP was inadequate, meaning that the Department did not have adequate processes and procedures in place for assuring and monitoring whether schools acted on its directive.

⁵ The TSSP was established in 1999 and provisions a weekly allocation of technical support hours to each government school. This allocation is determined based on student enrolments, with a minimum allocation for any school of 4 hours per week, for 46 weeks per year. Over 750 specialist technicians are engaged through the program.

25. Further, even once the data breach eventuated and was identified, the Department had difficulty communicating the response requirements to schools and/or in getting schools to act on the criticality of patching the vulnerability.
26. In summary, OVIC found that exposure to unpatched internet facing servers after a critical vulnerability was identified should have warranted greater attention by the Department.
27. The Department advised OVIC that as a result of this incident, it has identified a range of strategies to strengthen its Information Security Policy and the security controls associated with the TSSP.

Issue 2: Inadequate vulnerability management

28. The Department has threat intelligence processes in place to identify various types of vulnerabilities. One of its vendors identified the data breach the subject of this investigation through its routine security monitoring. Until this notification to the Department, the affected school was not aware that its network and servers had been breached.
29. A critical exploitable vulnerability is a severe software or hardware weakness likely causing massive operational disruption, data theft or unauthorised control.
30. Through its Vulnerability Management Program, the Department deploys technology to actively scan and report on vulnerabilities affecting schools.
31. However, OVIC found that not all schools are covered by the Vulnerability Management Program. Additionally, not all critical vulnerabilities identified are effectively remediated.
32. In summary, OVIC considers that the Vulnerability Management Program was not sufficient to adequately detect critical vulnerabilities affecting school servers.
33. OVIC notes the Department's intention to move to centrally provided technologies by the end of 2028. While this represents an opportunity for strengthened ICT governance and risk processes, the long lead time means that the Department must manage the remaining risks appropriately in the meantime.
34. The Department informed OVIC that since the cyberattack, it has deployed additional threat discovery tools that have reduced the likelihood of similar risks happening again.
35. Additionally, the Department has advised it will conduct an internal audit in 2027 to review the efficacy of its vulnerability management processes for schools.

Issue 3: Failure of the Information Security Policy Framework

36. Under the devolved schools model,⁶ it is the Department's role to set security policies and provide advice to schools through guidelines, while schools are responsible for implementing centrally defined security policies.
37. The Department has an Information Security Policy Framework which includes information security policies for school operations. The policy framework is owned by the Department's Chief Information Officer and governed by the Information Management and Technology Committee.
38. The Department's Information Security Policy for schools covers information relevant to planning and preparing for an information security incident.
39. The Department also has an Emergency and Critical Incident Management Planning Policy for schools, which was updated in August 2025. However, while the policy makes two passing references to cyber security, it is predominantly focused on physical threat events such as earthquakes, floods, fires, explosions, accidents and physical security threats.
40. In summary, OVIC found that the Department does not provide sufficient guidance to schools regarding planning and preparing for a major cyber security incident.
41. The Department advised OVIC that strengthened compliance requirements can be achieved by December 2026. However, the Department also advised that additional resourcing and budget for adequate oversight of the information security policy for school operations will be required.

Issue 4: Ineffective records management

42. IPP 4.2 requires organisations to take reasonable steps to destroy or permanently deidentify personal information when it is no longer needed for any purpose. IPP 4.2 helps to minimise the potential security risks that arise when information is retained for too long. One of the key reasons for disposing of outdated and unnecessary information is to remove the risk of inadvertent or unauthorised disclosure of that information.
43. OVIC considered whether it was reasonable for the Department to retain the personal information of hundreds of thousands of past students on its systems.
44. The Department told OVIC that it was essential to maintain the credentials of past students to ensure current students will not be issued the same email address which may give them

⁶ The devolved schools model, which is also known as 'school-based management', transfers key decision-making authority, including the day-to-day administration and operation of the school, to school leaders and councils.

access to the sensitive data of former students. However, OVIC found that the Department's practices were not a proportionate response to the business need it identified.

45. The Department advised OVIC that an archive policy for the removal of inactive student records will be developed by December 2026. However, it advised that additional funding and resourcing to implement the policy will be required.

What we concluded

46. The investigation found that the Department contravened both IPP 4.1 and IPP 4.2.
47. The Department had interfered with the privacy of students' information because its security controls were inconsistent with the requirements of IPP 4.1 and its record management practices were inconsistent with the requirements of IPP 4.2.

Recommendations

Vulnerability detection and patching policies and procedures

Recommendation 1:

That by 31 December 2026, the Department develop a plan to assess and align its security practices with the Australian Cyber Security Centre's Essential Eight requirements to ensure critical vulnerabilities are identified, prioritised and remediated within the required timeframes.

Recommendation 2:

That by 31 December 2026, the Department review and strengthen its processes for communicating critical zero-day exposures throughout the schools network and include a feedback loop to ensure schools are aware of and act on future security advisories.

Recommendation 3:

That by 31 December 2026, the Department review the efficacy of its vulnerability management processes for schools, including resourcing, coverage and effectiveness in identifying critical exploitable vulnerabilities, and remediation rates and timelines.

Information security policy and practices for school operations

Recommendation 4:

That by 31 December 2026, the Department establish processes and procedures for ensuring effective implementation and oversight of the information security policy for school operations.

Recommendation 5:

That by 31 December 2026, the Department revise the Emergency and Critical Incident Planning policy for schools to include a greater emphasis on cyber security incidents.

Recommendation 6:

That by 31 December 2026, the Department review and strengthen the obligations, governance, monitoring and assurance of the Technical Support for Schools Program.

Records management policies and procedures

Recommendation 7:

That by 31 December 2026, the Department review its policies and procedures around the retention of past students' credentials on its systems.

How the Department responded to the investigation

48. In correspondence to the Information Commissioner, the Department acknowledged the concerns identified through the investigation and accepted that stronger measures are required to provide the level of assurance necessary to safeguard the personal information of students effectively. It stated that while the Department has undertaken substantial work to strengthen privacy, cyber security and child safety arrangements, it recognises that further improvements are necessary.

49. The Department's full, formal response to the investigation report is provided at Appendix A.

Appendix A – The Department’s response



The Department of Education is committed to meeting its obligations under Victorian privacy law and to ensuring that appropriate governance arrangements, technologies and operational frameworks are in place to protect personal information across Victorian government schools.

The department welcomes and accepts the Victorian Information Commissioner’s recommendations to further strengthen existing initiatives, improve assurance and enhance the protection of personal information within Victorian government schools. The department has commenced implementation of the recommendations, noting that full implementation requires additional funding and resources, and will take time to deliver in a considered and effective way.

Over the past 4 years, the department has invested in the Securing Connected Learners program to maintain child-safe digital environments and in response to increasing cyber security risks. This investment is designed to strengthen the cyber security capability of Victorian government schools and to support a more secure and resilient technology environment.

The department is also undertaking significant work to transform school network environments to enable more consistent and centralised assurance in relation to security and child safety policy settings. This will support improved visibility, stronger oversight and a more consistent application of safeguards across school networks.

The department is confident that these initiatives are significantly improving cyber security capability across Victorian government schools. The department acknowledges the issues identified in this investigation and accepts that, in some areas, its existing arrangements have not been sufficient to provide the level of assurance required to safeguard personal information effectively.



www.ovic.vic.gov.au