CHECKLIST · SCAMS & SECURITY

Victorian schools data breach: regulator finds a missed patch and records kept too long

Published 10 October 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/victorian-schools-data-breach-ovic-report/

- [ ] **Ask for proof that urgent patches were applied.** When you or your IT provider send out a critical security notice, require a reply from each site or device owner saying it's done, and chase the ones that don't answer.
- [ ] **List every internet-facing server and who patches it.** Include servers at branches, franchise sites and anything an outside technician looks after.
- [ ] **Check what your vulnerability scanning covers.** Ask your IT provider which locations and systems it doesn't scan, and how quickly critical findings are fixed.
- [ ] **Find the accounts and records of people who have left.** Former customers, students, members and staff sitting in a live database are exposed in a breach too.
- [ ] **Set a rule for removing inactive records.** Decide how long each type is kept and who deletes or archives it, then put the first clean-up in the calendar.
- [ ] **Add a cyber incident to your emergency plan.** Write down who decides, who calls the IT provider and who tells the people affected.

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.