



CYBER SAFETY & E-CRIME POLICY

POLCY UPDATED June 2026

This policy provides a framework to promote cyber safety, ensure responsible online behaviour, and manage e-crime effectively to protect students, staff, and the broader school community.

Scope

This policy applies to:

- All employees, contractors, and visitors to the site, including teaching and non-teaching staff.
- Students enrolled at the site.
- Use of any ICT resources, personal devices, or online platforms within or outside school premises, where school-related activities are impacted.

Policy Details

1. Principles

1. Cyber safety is essential to maintaining a safe and conducive learning environment.
2. All members of the school community are responsible for engaging respectfully and safely in online spaces.
3. E-crime (cyberbullying, hacking, identity theft, etc.) will not be tolerated and may be referred to law enforcement as appropriate.

2. Roles and Responsibilities

For Staff:

- Educate students on responsible digital citizenship and cyber safety.
- Follow departmental protocols for responding to online safety incidents.
- Report all suspected e-crime or cyber safety breaches to the Site Leader or ICT Support Staff promptly.

For Students:

- Use ICT resources responsibly and ethically.
- Refrain from engaging in cyberbullying, hacking, or accessing inappropriate content.
- Report all cyber safety concerns to a teacher or appropriate staff member.

For Site Leaders:

- Implement department-specified procedures for managing online safety incidents.
- Coordinate with the ICT Cyber Security team when significant incidents occur.
- Ensure staff, students, and parents are informed of their responsibilities under this policy.

3. Managing Cyber Safety Incidents

1. Online Bullying & Harassment:

- Behaviour management policies apply to all bullying instances, including those occurring online.
- Incidents outside school hours are addressed when they impact the school environment or student wellbeing.



2. Inappropriate Content/Activities:

- Internet filtering systems will block harmful or objectionable content. Any attempts to bypass filters are strictly prohibited.
- Inappropriate use of departmental systems will be subject to disciplinary action.

3. E-Crime (Reportable Offences):

- Severe incidents (e.g., threats, sensitive data breaches) must be reported in the Critical Incident Reporting System (IRMS) within 24 hours.
- Suspected e-crime impacting personal safety or finances must involve ICT Cyber Security and, if necessary, South Australia Police (SAPOL).

4. Reporting and Escalation

- All incidents must be logged, escalated, and resolved as outlined in the Cyber Security Incident Response Procedure.
- ICT Cyber Security will classify cases into Low, Moderate, High, or Critical and allocate resources accordingly.
- Severe cases (e.g., media coverage or inter-agency responses) will involve the Incident Management Directorate.

5. Education and Awareness

- The school will integrate cyber safety education into the curriculum using resources like the [Office of the eSafety Commissioner](#).
- Parent information sessions will promote conversations about online safety at home.

6. Consequences for Breaches

- Students may face disciplinary actions ranging from the loss of ICT privileges to suspension.
- Staff whose conduct conflicts with cyber safety expectations may face disciplinary action per departmental guidelines.
- Criminal behaviour will be referred to SAPOL.

Related Documents and Policies

1. [Responding to Online Safety Incidents in South Australian Schools Guidelines](#)
2. [ICT Cyber Security Standard](#)