Student Duty of Care

Cyber Safety Policy and Procedures

Policy Introduction

We are committed to meeting our Student Duty of Care obligations.

Purpose

This Policy sets out how St Mary's School, Echuca manages cyber safety issues.

Cyber safety issues most commonly occur through a children and young person’s use of their own technology devices (e.g. smart phone, tablet, laptop, home computer).

Scope

This Policy applies to all staff, volunteers and contractors at the school.

Roles and Responsibilities

Staff Responsibilities

All staff must:

- model appropriate online behaviour at all times

- refer any cyber safety related issues to the Cyber Safety Primary Contacts
- acknowledge the right of parents/carers to speak with school authorities if they believe their child is being bullied.

Policy Statement

St Mary's School, Echuca recognises its duty to children and young persons to provide a safe and positive learning environment which includes the responsible use of information and communication technologies.

It is our policy that:

- cyber safety be managed through a “whole-of-school community” approach involving children and young persons, staff and parents/carers
- cyber safety and cyberbullying prevention strategies be implemented within the school on a continuous basis with a focus on teaching age-appropriate skills and strategies to empower staff, children and young persons and parents/carers to recognise cyber safety issues and respond appropriately
- cyberbullying response strategies be tailored to the circumstances of each incident
- our bullying prevention, intervention and cyber safety strategies are reviewed on an annual basis against best practice.

Procedures

Cyber Safety Strategies

St Mary's School, Echuca recognises that the implementation of whole of school cyber safety strategies is the most effective way of minimising risks related to our children and young persons engaging in online activity.

The following initiatives form part of our overall cyber safety strategy within the school:

- a structured curriculum and peer group support system, that provides age-appropriate information and skills relating to cyber safety (including cyberbullying) to children and young persons over the course of the academic year
- education, training and professional development of staff in cyber safety strategies
- regular provision of information to parents/carers to raise awareness of cyber safety as a school community issue. This will equip them to recognise signs of cyber safety risks, as well

as to provide them with clear paths for raising any concerns they may have relating to cyber safety and/or cyberbullying directly with the school
- promotion of a supportive environment that encourages the development of positive relationships and communication between staff, children and young persons and parents/carers
- promotion of responsible bystander behaviour amongst children and young persons, staff and parents/carers (this may occur where a bystander observes inappropriate online behaviour either being perpetrated by, or targeted at, a children and young person
- regular risk assessments of cyber safety within the school are undertaken by surveying children and young persons to identify cyber safety issues
- records of reported cyber safety incidents are maintained and analysed, in order to identify systemic issues and to implement targeted prevention strategies where appropriate
- cyber safety strategies are included in children and young persons' school diaries
- cyber safety posters are displayed strategically within the school
- promotion of children and young person cyber safety awareness by participating in relevant cyber safety related events.

Implementation

This Policy is implemented through a combination of:

- staff training
- children and young person and parent/carer education and information
- effective incident reporting procedures
- effective management of cyber safety incidents when reported
- the creation of a "no bullying" culture within the school community
- effective record keeping procedures
- initiation of corrective actions where necessary.

Definitions

Cyber safety refers to the safe and responsible use of information and communication technologies. This includes privacy and information protection, respectful communication and knowing how to get help to deal with online issues.

Common cyber safety issues include:

- **Cyberbullying** - the ongoing abuse of power to threaten or harm another person through the use of technology (Refer to our Bullying Prevention and Intervention Policy and Procedures)
- **Sexting** - the sending or posting of provocative or sexual photos, messages or videos online
- **Identity theft** - the fraudulent assumption of a person's private information for personal gain. Children and Young Persons are exposed to these risks as they are often unaware of the safety issues surrounding their digital footprint
- **Predatory behaviour -** where a children and young person is targeted online by a stranger who attempts to arrange a face-to-face meeting, in an attempt to engage in inappropriate behaviour.

Related Policies

- Bullying Prevention and Intervention Policy and Procedures
- Information and Communication Technology (ICT) Policy and Procedures

Policy Administration

This policy is scheduled for review 3 yearly or more frequently where appropriate. All policies have been reviewed and approved by the relevant Executive Leadership Team member.

Reviewed date: 2025