St. Mary's School
ECHUCA

Student Duty of Care

Children and Young Person Use of Social Media Policy and Procedures

Policy Introduction

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

Purpose

The purpose of this Policy is to set standards of behaviour for the use of social media that are consistent with the broader values and expectations of the school community.

Scope

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

Roles and Responsibilities

The Principal and Management/Executive Team are responsible for the effective implementation of this Policy.

Policy Statement

St Mary's School, Echuca recognises the importance of social media tools as a mechanism for both individuals and organisations to engage and share information.

Children and Young Persons at the school enjoy the opportunities and rewards that being a member of the school community brings. It is subsequently expected that children and young persons will uphold the ethos of the school within and outside of the school and in all social media interactions.

It is our policy that children and young persons must:

- use social media in a respectful and responsible manner
- refrain from acting in such a way that brings the school into disrepute or in a way that harms members of the school or wider community
- not insult or present offensive or inappropriate content
- not misrepresent the school or any member of the school community.

Social Media Code of Conduct

Children and Young Persons are expected to show respect to others, including members of the school and wider community. Children and Young Persons are also expected to give due respect to the reputation and good name of the school.

When using social media, children and young persons are expected to ensure that they:

- respect the rights and confidentiality of others
- do not impersonate or falsely represent another person
- do not use avatars or other means of hiding or misrepresenting their identity
- do not bully, intimidate, abuse, harass or threaten others
- do not make defamatory comments
- do not use offensive or threatening language or resort to personal abuse towards each other or members of the school or wider community
- do not post content that is hateful, threatening, pornographic or incites violence against others
- do not harm the reputation and good standing of the school or those within its community
- do not film, photograph or record members of the school community without express permission of the school or use film, photographs or recordings without express permission of the other parties.

A failure to abide by the above expectations may constitute bullying. For more information, refer to our Bullying Prevention and Intervention Policy and Procedures.

Procedures

Privacy Risks and Preventative Strategies

New technologies change the way children and young persons share personal information. As a result, social media sites present new privacy risks.

If a social media entity is covered under the Privacy Act 1988 (Cth), the way they collect and use user information must be compliant with their obligations under the Australian Privacy Principles (refer to our Privacy Program).

In relation to social media use, the following privacy risks arise:

- users may not have control over who sees the personal information they share online
- social media sites permanently archive personal information, even after users deactivate their accounts
- users may have their online posts republished by other users, an act over which they often have little control
- users open themselves up to personal and professional reputational damage as a result of social media over-sharing
- users open themselves up to online identity theft which often leads to serious financial and reputational damage.

To protect their privacy online, children and young persons are advised to:

- personally adjust the privacy settings on their social media pages
- only add people that they know and trust as online friends and contacts
- protect their accounts with strong passwords
- not access social media sites by clicking a link provided in an email or on another website
- disable ‘geo-tagging’ or location information sharing on social media accounts and mobile devices to prevent strangers from knowing their personal home or school locations
- avoid ‘checking in’ at personal locations, such as their home, the school, other people’s homes or while on excursions
- limit the amount of personal information (e.g. date of birth, address, information about your daily routine, holiday plans etc.) they provide on social media sites to prevent identity crime.

Identity Crime Risks and Preventative Strategies

Identity crime is another risk of social media use. Identity crime describes the criminal use of another person's identity to facilitate in the commission of a fraudulent act.

Children and Young Persons bear the risk of identity crime when they share personal information on social networking sites. Online identity theft has become more prevalent over the years, particularly as more and more users create online accounts and publicly share personal information.

The consequences of identity theft can include:

- personal and professional reputational damage
- physical harm
- substantial financial loss (e.g. credit card fraud).

Children and Young Persons are advised to be cautious of the personal information that they share online. Extreme care should be taken when providing personal details such as date of birth, address, phone contacts or educational details.

When in doubt, children and young persons are advised to use the most secure privacy setting on their social media pages.

Reputational Risks and Preventative Strategies

Whenever users communicate through social media, their comments and posts are viewable by a large audience. In this way, all online communications will reflect on the user and their reputation. While this digital representation may have negative repercussions on the children and young person, the school may also be vicariously affected.

In order to avoid reputational damage, children and young persons are advised to:

- remove content that may negatively reflect on them or the school
- think before they post and reflect on the potential harm the post may pose
- gain permission from the school before publicly sharing school information
- adjust their online security profile to limit the people who can see their personal information.

Breach

Breaches to this Policy may result in disciplinary action in line with CESL policies and legislative obligations.

Definitions

Term	Definition
Social media	Social media refers to online tools which provide individual users and/or organisations with the ability to create and share content in online communities. Social media tools include, but are not limited to, the following: • Social Networking Sites – such as Facebook, LinkedIn, Instagram, Snapchat, Pinterest, TikTok, Discord • Video/Photo Sharing Sites – such as YouTube, Flickr, TikTok, Instagram, Snapchat, Tumblr • Micro-Blogging Sites – such as X, Yammer, Yahoo Buzz, Reddit • Weblogs – corporate, personal or media blogs published through tools such as Wordpress • Forums and Discussion Boards – Whirlpool, Yahoo! Groups, Google Groups • Geo-spatial Tagging – such as Foursquare • Online Multiplayer Gaming Platforms – such as Second Life • Instant Messaging – SMS, WeChat, WhatsApp, Facebook Messenger • Vodcasting and Podcasting • Online Encyclopaedias - such as Wikipedia • Any other websites or devices (including mobile phones) that enable individuals to publish or distribute their own views, blogs, comments, photos, videos etc.
Sexting	Sexting is the sending or posting of provocative or sexual photos, messages or videos online. Sexting is treated differently under federal and state or territory laws but in general, sexting will constitute criminal conduct when it involves children and young persons aged under 18 and when it involves harassment or bullying. The creation and/or distribution of the images may constitute child pornography. Where sexting involves minors, the Police should be notified. For more information, refer to our Cyber Safety Policy and Procedures and Harassment (Student Against Student) Policy and Procedures.

-

Related Policies

- Bullying Prevention and Intervention Policy and Procedures
- Information and Communication Technology (ICT) Policy and Procedures
- Cyber Safety Policy and Procedures
- Student Use of Mobile Devices Policy and Procedures
- Harassment (Student Against Student) Policy and Procedures
- Privacy Program

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