Social Media Policy

Rationale

St John's Grammar School seeks to provide and promote a safe and productive learning environment for all students. As such, this policy and associated procedures seek to promote student wellbeing, safe and responsible use of digital technologies, and the development of skills and behaviours that foster learning, responsibility and positive behaviours. 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.

St John's Grammar School's Policy

St John's Grammar School recognises the importance of social media tools as a mechanism for both individuals and organisations to engage and share information. Students, staff, parents and other members of the School community enjoy the opportunities and rewards that being a member of the School community brings. It is subsequently expected that all members of our community will uphold the ethos of the School within and outside of the School and in all social media interactions.

It is our policy that all members of our community will:

- 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 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

Students, staff and parents are expected to show respect to others, including members of the School community, and are also expected to give due respect to the reputation and good name of the School.

When using social media, students and staff 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 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.

Privacy Risks and Preventative Strategies

New technologies change the way students, staff and parents 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.

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, students 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. Students 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).

Students 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, students 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 student, the School may also be vicariously affected.

In order to avoid reputational damage, students 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.

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 students 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.

Refer to our Cyber Safety and Harassment (Student Against Student) policies.

Related Policies

- Anti-bullying Policy
- Mobile Phone Policy
- Behaviour Policy
- ICT Acceptable Use Policy
- Cyber Safety Policy