Mansfield Steiner School Online Conduct and Cyber Safety Policy – Further Guidance Document

This Policy should be read in conjunction with the policy found on the school's Policy Connect Portal

https://mansfieldrudolfsteiner.policyconnect.com.au/module/223/page/7cce54d3-324a-4922-b3a4-43bd27a4049d.md

1. Introduction

Mansfield Steiner School recognizes the significance of social media tools as a means for individuals and organizations to engage and share information. This policy aims to establish standards of behaviour for the use of social media that align with the values and expectations of the School community.

2. Student Use of social media

2.1 Definition of social media

Social media encompasses various online tools that enable users to create and share content within online communities. These tools include, but are not limited to, the following:

- Social Networking Sites: Facebook, LinkedIn, Instagram, Snapchat, Pinterest, TikTok, Discord
- Video/Photo Sharing Sites: YouTube, Flickr, TikTok, Instagram, Snapchat, Tumblr
- Micro-Blogging Sites: Twitter, Yammer, Yahoo Buzz, Reddit
- Weblogs: Corporate, personal, or media blogs published through platforms like Wordpress
- Forums and Discussion Boards: Whirlpool, Yahoo! Groups, Google Groups
- Geo-spatial Tagging: Foursquare
- Online Multiplayer Gaming Platforms: Second Life
- Instant Messaging: SMS, WeChat, WhatsApp, Facebook Messenger
- Vodcasting and Podcasting
- Online Encyclopedias: Wikipedia
- Any other websites or devices (including mobile phones) enabling individuals to publish or distribute their views, blogs, comments, photos, videos, etc.

2.2 Policy Objectives

- Students must use social media respectfully and responsibly.

- Students should avoid engaging in actions that bring the School into disrepute or harm members of the School community.
- Insults, offensive or inappropriate content, and misrepresentation of the School or its members are prohibited.
-

3. Social Media Code of Conduct

Students are expected to abide by the following guidelines when using social media:

- Respect others' rights and maintain confidentiality.
- Refrain from impersonating or falsely representing another person.
- Avoid using avatars or other means to hide or misrepresent their identity.
- Do not engage in bullying, intimidation, abuse, harassment, or threats towards others.
- Refrain from making defamatory comments.
- Do not use offensive or threatening language or resort to personal abuse towards each other or School community members.
- Do not post hateful, threatening, pornographic, or violent content.
- Protect the reputation and standing of the School and its community.
- Do not film, photograph, or record members of the School community without express permission, and do not use such media without proper consent.

Failure to comply with these expectations may be considered bullying, and the School's Bullying Prevention and Intervention policy will apply.

4. Privacy Risks and Preventative Strategies

Using social media involves privacy risks, and students are advised to take precautionary measures to protect their privacy:

- Adjust privacy settings on social media pages to control who can view personal information.
- Add only known and trusted individuals as online friends or contacts.
- Use strong passwords to secure accounts.
- Avoid accessing social media sites through links provided in emails or on other websites.
- Disable geo-tagging or location sharing to prevent strangers from knowing personal home or School locations.

- Refrain from "checking in" at personal locations like home, School, or others during excursions.
- Limit the amount of personal information provided on social media to prevent identity crime.

5. Identity Crime Risks and Preventative Strategies

Sharing personal information on social media poses the risk of identity crime. To mitigate this risk:

- Exercise caution when sharing personal details like date of birth, address, phone contacts, or educational information.
- Use the most secure privacy settings available on social media pages when unsure.

6. Reputational Risks and Preventative Strategies

Online communications through social media can impact an individual's reputation and also reflect on the School. To avoid reputational damage:

- Remove content that may negatively reflect on oneself or the School.
- Think before posting and consider the potential harm the post may cause.
- Obtain permission from the School before publicly sharing School information.
- Adjust online security profiles to limit the audience who can view personal information.

7. Sexting

Sexting, involving the sending or posting of provocative or sexual photos, messages, or videos online, may constitute criminal conduct, especially when it involves students under 18 or harassment/bullying. The creation and distribution of such images may be considered child pornography. Incidents involving minors should be reported to the Police.

Refer to the School's Cyber Safety and Harassment policies for more information.

8. Implementation

This Policy will be implemented through the following measures:

- Staff training
- Student and parent/carer education and information
- Effective incident reporting procedures
- Proper management of reported bullying incidents

- Maintenance of comprehensive records
- Initiation of corrective actions when necessary
- The Principal's responsibility for overseeing the policy's effective implementation

9. Breach of Policy

A breach of this policy may also involve a violation of other School policies. The following policies should be read in conjunction with this policy:

- Cyber Safety
- Information & Communication Technology (ICT)
- Student Use of Mobile Devices
- Bullying Prevention and Intervention

Breach of this policy will be assessed on a case-by-case basis by the Principal. Reports of cyberbullying, hacking, and technology misuse will be fully investigated and may result in Police notification. Sanctions for students may include loss of computer privileges, detention, suspension, or expulsion from the School. In certain cases involving criminal activity, students and parents/carers may be subject to a criminal investigation by the Police, outside the control of the School.

Review date June 2023 Glenn Hood – Sent to GC June 2023

Next review June 2024