Doctrina Vitae

Bacchus Marsh
Grammar

# School Policy

## Student Duty of Care

### Student Use of Social Media Policy

(source: Complispace)

Approved by the School Principal 18 March 2022

# Student Use of Social Media Policy

# 1 Social Media

1.1.1 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, Tik Tok
- Video/Photo Sharing Sites – such as YouTube, Flickr, Tik Tok, Instagram, Snapchat, Tumblr
- Micro-Blogging Sites – such as Twitter, Yammer, Yahoo Buss, Reddit
- Weblogs – corporate, personal or media blogs published through tools such as Wordpress
- Forums & 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.

# 2 Bacchus Marsh Grammar's Policy

2.1.1 Bacchus Marsh Grammar recognises the importance of social media tools as a mechanism for both individuals and organisations to engage and share information.

2.1.2 Students at the School enjoy the opportunities and rewards that being a member of the School community brings. It is subsequently expected that students will uphold the ethos of the School within and outside of the School and in all social media interactions.

2.1.3 It is our policy that students must:

2.1.3.1 Use social media in a respectful and responsible manner

2.1.3.2 Refrain from acting in such a way that brings the School into disrepute or in a way that harms Members of the School community

2.1.3.3 Not insult or present offensive or inappropriate content

2.1.3.4 Not misrepresent the School or any member of the School community.

# 3 Rationale

3.1.1 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.

# 4 Social Media Code of Conduct

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

4.1.2 When using social media, students are expected to ensure that they:

4.1.2.1 Respect the rights and confidentiality of others

4.1.2.2 Do not impersonate or falsely represent another person

4.1.2.3 Do not use avatars or other means of hiding or misrepresenting their identity

4.1.2.4 Do not bully, intimidate, abuse, harass or threaten others

4.1.2.5 Do not make defamatory comments

4.1.2.6 Do not use offensive or threatening language or resort to personal abuse towards each other or members of the School community

4.1.2.7 Do not post content that is hateful, threatening, pornographic or incites violence against others

4.1.2.8 Do not harm the reputation and good standing of the School or those within its community

4.1.2.9 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

4.1.2.10 Do not upload or circulate photos or videos of Bacchus Marsh Grammar students.

4.1.3 A failure to abide by the above expectations may constitute bullying. Refer to our Bullying Prevention and Intervention policy.

## 5 Privacy Risks and Preventative Strategies

5.1.1 New technologies change the way students share personal information. As a result, social media sites present new privacy risks.

5.1.2 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).

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

5.1.3.1 Users may not have control over who sees the personal information they share online

5.1.3.2 Social media sites permanently archive personal information, even after users deactivate their accounts

5.1.3.3 Users may have their online posts republished by other users, an act over which they often have little control

5.1.3.4 Users open themselves up to personal and professional reputational damage as a result of social media over-sharing

5.1.3.5 Users open themselves up to online identity theft which often leads to serious financial and reputational damage.

5.1.4 To protect their privacy online, students are advised to:

5.1.4.1 Personally adjust the privacy settings on their social media pages

5.1.4.2 Only add people that they know and trust as online friends and contacts

5.1.4.3 Protect their accounts with strong passwords

5.1.4.4 Not access social media sites by clicking a link provided in an email or on another website

5.1.4.5 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

5.1.4.6 Avoid 'checking in' at personal locations, such as their home, the School, other people's homes or while on excursions

5.1.4.7 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.

## 6 Identity Crime Risks and Preventative Strategies

6.1.1 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.

6.1.2 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.

6.1.3 The consequences of identity theft can include:

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

6.1.4 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.

6.1.5 When in doubt, students are advised to use the most secure privacy setting on their social media pages.

## 7 Reputational Risks and Preventative Strategies

7.1.1 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.

7.1.2 In order to avoid reputational damage, students are advised to:

7.1.2.1 Remove content that may negatively reflect on them or the School

7.1.2.2 Think before they post and reflect on the potential harm the post may pose

7.1.2.3 Gain permission from the School before publicly sharing School information

7.1.2.4 Adjust their online security profile to limit the people who can see their personal information.

## 8 Sexting

8.1.1 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.

8.1.2 For more information, refer to our Cyber Safety and Harassment policies.

## 9 Implementation

9.1.1 This policy is implemented through:

- Staff training
- Student and parent/guardian education and information
- Effective incident reporting procedures
- Effective management of bullying incidents when reported
- Effective record keeping procedures
- Initiation of corrective actions where necessary, and
- Allocation of the overall responsibility for the effective implementation of this policy to the Principal.

## 10 Breach of Policy

10.1.1 A breach of this policy may also involve a breach of other School policies, and this policy should be read in conjunction with our:

- Cyber Safety policy
- Information & Communication Technology (ICT) policy
- Student Use of Mobile Phones policy, and
- Bullying Prevention and Intervention policy.

10.1.2 A breach of this policy will be considered by the School and will be dealt with on a case by case basis.

10.1.3 All reports of cyber bullying, hacking and other technology misuses will be investigated fully and may result in a notification to Police where the School is obliged to do so.

10.1.4 Sanctions for students may include, but are not limited to, the loss of computer privileges, detention, suspension, or expulsion from the School.

10.1.5 Students and parents/guardians must be aware that in certain circumstances where a crime has been committed, they may be subject to a criminal investigation by Police over which the School will have no control.

## 11 Authorisation

| | | |
|---|---|---|
| **School Document No.** | | |
| **School Document Name** | **Student Use of Social Media Policy** | |
| **Approval Authority** | **Principal** | |
| **Approval Signature** | Andrew Neal<br>**Principal**<br>**Bacchus Marsh Grammar** | |
| **Administrator** | **Company Secretary** | Greg Gough |
| **Approval Date** | **18 March 2022** | |
| **Date of Next Review** | **18 March 2024** | To be reviewed every two years |

## 12 History

| **Date** | **Amendment** |
|---|---|
| **9 May 2017** | 1. New Policy |
| **26 February 2019** | 2. Reviewed |
| **11 November 2020** | 3. Reviewed |
| **18 March 2022** | 4. Reviewed and updated examples of social media |