Doctrina Vitae

Bacchus Marsh Grammar

POLICY

Social Media – Student Usage Policy

Approved: 09/05/2017

Bacchus Marsh Grammar
South Maddingley Road, Victoria
Mailing Address
PO Box 214
Bacchus Marsh, Vic 3340

CRICOS No:02911M
Reg. No:1919
ABN: 24 128 531 078
Email: school@bmg.vic.edu.au
Website: www.bmg.vic.edu.au

1 The Hazard – 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, Google+, Instagram, Snapchat, Pinterest
- Video/Photo Sharing Sites – such as YouTube, Flickr
- Micro-Blogging Sites – such as Twitter, Yahoo Buzz, Meme
- Weblogs – corporate, personal or media blogs published through tools such as Wordpress and Tumblr
- Forums & Discussion Boards – Whirlpool, Yahoo! Groups, Google Groups
- Geo-spatial Tagging – such as foursquare
- Online Multiplayer Gaming Platforms – such as second life
- Instant Messaging – including SMS
- Vod and Podcasting
- Online Encyclopaedias – 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

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

Students at Bacchus Marsh Grammar 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.

It is our policy that students and staff 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, present offensive or inappropriate content; and
- not misrepresent the School or any member of the School community.

3 Rationale

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

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.

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

4.1.1 Respect the rights and confidentiality of others;
4.1.2 Do not impersonate or falsely represent another person;
4.1.3 Do not use avatars or other means of hiding or misrepresenting their identity;
4.1.4 Do not bully, intimidate, abuse, harass or threaten others;
4.1.5 Do not make defamatory comments;
4.1.6 Do not use offensive or threatening language or resort to personal abuse towards each other or members of the School community;
4.1.7 Do not post content that is hateful, threatening, pornographic or incites violence against others;
4.1.8 Do not harm the reputation and good standing of the School or those within its community; and
4.1.9 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.
4.1.10 A failure to abide by the above expectations may constitute bullying. Refer to: Bullying Prevention & Intervention (all other states)

5 Privacy Risks and Preventative Strategies

The advent of new technologies changes the way both staff and students 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; or
- Users open themselves up to online identity theft which often leads to serious financial and reputational damage.

In order to protect their privacy online, students and staff 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, school or workplace locations;
- Avoid ‘checking in’ at personal locations, such as their home, the School, work, other people’s home or while on excursions; and
- 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

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 and staff 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; or
- Substantial financial loss (e.g. credit card fraud).

Students and staff 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, educational details etc.

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

7 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 staff member or student, the School may also be vicariously affected.

In order to avoid reputational damage, students and staff 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; and
- Adjust their online security profile to limit the people who can see their personal information.

8 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.

See the School's Cyber Safety Policy and Harassment (Student Against Student) Policy.

9 Implementation

This Policy is implemented through a program of:

- 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 should be read in conjunction with the:

- Cyber Safety Policy;
- Information & Communication Technology (ICT) Policy;
- Student Use of Mobile Phones Policy; and
- NSW Clients: Bullying Prevention & Intervention Policy.
- Other clients: Bullying Prevention & 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 Where a staff member breaches this Policy. the School will take disciplinary action, including in the case of serious breaches, summary dismissal.
10.1.6 Students and parents 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 Related Policies

Cyber Safety
Information & Communication Technology (ICT)
Student Use of Mobile Phones
Bullying Prevention & Intervention (NSW)
Bullying Prevention & Intervention (all other states)
Harassment (Student Against Student)

12 Resources

•The Office of the Children's eSafety Commissioner

13 Authorisation

Council Document Name	Social Media – Student Usage Policy	
Approval Authority	Principal	
Administrator		
Approval Date	09/05/2017	
Effective Date [Current version if different from amended date]	09/05/2017	
Amendment History		
Date of Next Review	09/05/2017	