Social Media Policy

Definition of key terms:

Social media is any form of online or web-based publication, forum or presence that allows interactive communication, including, but not limited to, Facebook, LinkedIn, Instagram, Snapchat, blogs, forums, discussion boards, chat rooms, Wikis, Twitter and YouTube.

Rationale

The purpose of this policy is to encourage acceptable and beneficial use of social media by staff and students and for community purposes at Holy Spirit Primary School, Thornbury East.

It is recognised that most employees may use or interact with social media at work and in a personal context and that social media plays an increasingly important role in the life-worlds of our students.

There is great potential for the use of social media in school communities in terms of educational outcomes and as a means of communication.

However, it is important that staff and community members understand the expectations of the School when using social media as there are risks that must be appropriately managed.

This policy directly relates to the requirements of the Child Safe Standards.

Related Policies

The Social Media Policy has linkages to other relevant School policies and professional expectations, for example:

- ICT User Agreement and Cybersafety Policy (incorporating the Working Online Policy)
- Anti-Bullying Policy
- Privacy Policy
- Victorian Teaching Profession Code of Conduct issued by the Victorian Institute of Teaching
- Holy Spirit Codes of Conduct for staff and parents

Social Media Risks

The following are some of the major risks associated with the use of social media:

- reputational damage to organisations and people;
- disclosure of confidential information and breach of privacy laws;
- posting of offensive, bullying, harassing, and discriminatory material;
- misuse of intellectual property and breach of copyright laws; and
- (for teachers) breaching the *Victorian Teaching Profession Code of Conduct* issued by the Victorian Institute of Teaching.

Guiding Principles

Users must recognise:

- online behaviour should at all times demonstrate respect for the dignity of each person;
- the need to behave in an ethical manner when using social media (even for personal communication) as those communications can reflect on their role at the school and must be consistent with the Catholic beliefs and ethos of the school and professional expectations and standards;
- social media activities may be visible to current, past or prospective staff, students and parents.

Further principles for staff members:

Staff must recognize:

Employees will avoid the potential of breaching this policy and compromising the professional expectations of them at the school if they do not use personal social media forums to:

- post any material about the school (eg. students, parents, policies, employees etc); or
- post inappropriate material about themselves; or
- make inappropriate contact with members of the school community (this point is explained further later in the policy)

School-related use of Social Media

The use of social media for educational or communication purposes must be in accordance with other relevant School policies and procedures relating to online learning and privacy .

Generally

When using social media for school-related purposes, users must:

- first obtain the consent of the Principal (which can be for a specific instance or for a general purpose or role) before:
    - posting any material that may be perceived as being made "on behalf" of the School (eg. any commentary, School information, photographs of the School, students, staff or other identifying images); and
    - using the School's logo, trademarks, official photographs or any other intellectual property of proprietary materials; and
- not post inappropriate material or commentary that breaches other policies or guidelines
- obtain the explicit permission of individuals (or parents) before posting images/video of community members

If there are reasonable concerns that posting any material could be considered inappropriate (eg. in light of potential privacy or copyright obligations), then an employee must first raise those concerns with the principal or a delegate of the principal before posting the material.

Community accounts (such as those overseen by the HSPA) need to have the principal or a delegate of the principal as a 'co-administrator' of the account.

Students use of Social Media

Students are not permitted to log into non-school related, personal social media accounts at school.

Any use of social media at school is governed by the ICT User Agreement and Cybersafety Policy and must have an explicit learning purpose.

Students' safe use of social media at home will be supported by an explicit cybersafety program at school.

Unsafe, mean, bullying or harassing behaviours that occur using personal social media or email accounts that affect school community members may be addressed under the school ICT User and Cybersafety agreement.

Parental use of Social Media

There is an expectation that parents will refrain from mean, bullying or harassing behaviours towards other community members on social media. The school recognizes a potential need to intervene should such behavior occur.

Personal use of Social Media for Staff

Generally

It is recognised that employees may use social media in their personal life. However, it is also recognised that such use may impact on the employment relationship.

Accordingly, employees' personal use of social media must:

- not bring the School into disrepute or interfere with, or compromise their duties or responsibilities to the School or students;
- comply with other policies of the School and professional standards that outline expected behaviours of employees when posting personal comments that relate to, or can be identified as relating to, School issues (eg. discussing or referencing employees, students, policies or anything related to, or reflecting upon the School); and
- take steps to ensure that friends, family or other acquaintances are aware of the need to use discretion when they post images or information about the employee on their own social media forums.

To avoid potentially breaching this policy or compromising the professional expectations of them as employees at the School, it is recommended that employees' use of social media not involve connections with the following persons on social media forums (for example, being "friends" on Facebook):

- recent former students (ie. enrolled at the School within a two year period before connecting); or
- parents of current students;

unless special circumstances exist (eg. a parent is a personal friend or former student is a relative) and the employee has advised the Principal of the connection and the circumstances.

Students

Employees must NOT connect with students or interact with, or post images of, students on their own private social media forums (for example, employees must not be "friends" with students on Facebook).

An exception to this requirement is when prior approval for the connection has been obtained from the Principal on the basis that an employee and a student will appropriately interact within the valid context of a legitimate purpose (for example, both are family members/relatives or both are members of a community sporting team and interactions are purely for the purpose of participating in that sport).

Security, Privacy and Access

To avoid potentially breaching this policy or compromising the professional expectations of them as employees at the School, it is recommended that employees:

- ensure the privacy settings of their social media profiles are appropriately set to avoid putting their privacy at risk (for example, minimum recommendation for Facebook accounts: settings set to "only friends" and NOT "Friends of Friends" or "Networks and Friends" as these open your content to a large group of unknown people); and
- recognise that even if they implement the maximum security settings for their social media profiles, the security settings on social media forums cannot guarantee that communications placed online do not become more publicly available than was intended (employees should always assume that posts or communications online may become public).

Employees must understand that the type of security settings used cannot excuse breaches of this policy if the material posted is inappropriate and becomes more publicly available than was intended.

Consequences of Breaching this Policy

Non-compliance with this policy may be grounds for disciplinary action. Depending on the seriousness of the circumstances, disciplinary action can be up to and including termination of employment.

Policy Review

This Policy will be reviewed every two years to take account of any changed technology, legislation, expectations or practices.

Date of last review – October 2016