Berry Street School
Social Media and eSafety Policy

1   Purpose

The purpose of this policy is to ensure that social media and on-line use at the Berry Street School is safe, supportive and protects all stakeholders from intentional and unintentional on-line harm.

2   Definitions

Word / term / phrase	Definition
Social media	All forms of electronic communication through which users create on-line communities to share information, ideas, personal messages and other content (e.g. videos) Social media encompasses (but is not limited to); • Social networks (e.g Facebook, LinkedIn) • Video sharing (e.g. YouTube, TikTok, Facebook Live) • Photo sharing (e.g. Instagram, Snapchat, Pinterest) • Microblogging (e.g. Twitter, Plurk) • Blogging and forums (e.g. Medium, Tumblr) • Social review sites (e.g. TripAdvisor, Yelp, Foursquare) • Bookmarking sites (e.g. Pinterest, Flipboard)
Personal information	Under the Privacy Act 1998 (Cwth), personal information is defined as: information or an opinion about an identified individual, or an individual who is reasonably identifiable – whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not

3   Scope

This policy applies to all students, teachers and staff at the Berry Street School. School staff are issued with Berry Street devices (laptops and mobile phones) therefore this policy applies to both personal and Berry Street issued devices.

This policy does not cover the personal use of social media by other Berry Street employees, volunteers or carers, please refer to the *Personal Use of Social Media Policy.*

This policy does not cover the use of social media within service delivery and carer support, please refer to the *Social Media and eSafety within Service Delivery Policy.*

4   Review Cycle

The Social Media and eSafety Policy will be reviewed every three years in line with the Plan Do Check Act cycle, and as outlined in the Policy Framework.

5   Background and Context

Social media is an increasingly popular and important part of people's lives, enabling greater connection and communication with others, or as a source of information and entertainment. (please refer to Section 2 of this policy for a definition and examples of social media applications).

While social media has enabled new opportunities for people to express themselves and communicate with others, it also creates more risk, particularly for children and young people.

Importantly, the limitations of government regulation with respect to the architecture of social media platforms and behaviour of social media account holders, requires the end user to be fully informed and cautious regarding their registration, chosen privacy settings and use.

6   Policy

6.1   Personal use of social media

While the Berry Street School acknowledges people's rights to freedom of expression, students, teachers and staff also have a responsibility not to breach the privacy rights or make comment regarding other members of the Berry Street School community.

The School requires students, teachers and staff to consider the potential impact of what is being communicated or shared via social media and on-line environments at all times, including;

- Never identify, make comment, or breach the privacy of other students, teachers or staff;
- Never take any photos or videos while at school or post photos or videos of students, teachers or staff on social media;
- Never post content that may damage the reputation of Berry Street or the Berry Street School;
- Never make obscene, defamatory, threatening, harassing, discriminatory or hateful comments.

Similar to other schools, the strong expectation for all students, teachers and staff is that personal use of social media while at school does not occur during school hours and does not interfere with school commitments.

Teachers and staff must not use their personal social media accounts to initiate contact or respond to social media comments or direct contact made by students, parents, guardians or carers.

6.2 Supporting students to use social media and on-line environments safely

The Berry Street School supports and promotes the safe use of social media for students outside of school hours. This can be achieved by students, teachers and familes/carers being aware of and discussing the risks, and to quickly identify any warning signs.

The Australian eSafety Commissioner has identified that the main social media risks for children and young people are cyberbullying, sexting, unwanted contact and on-line grroming.

6.2.1 Cyberbullying

Cyberbullying behaviour takes many forms, such as sending abusive messages, hurtful images or videos, nasty online gossip, excluding or humiliating others, or creating fake accounts in someone's name to trick or humiliate them. Warning signs of cyberbullying include;

- being upset after using the internet or mobile phone.
- changes in personality e.g. becoming more withdrawn, anxious, sad, angry.
- appearing more lonely or distressed.
- unexpected changes in friendship groups.
- a decline in schoolwork, hobbies and interests.
- changes in sleep patterns.
- a decline in physical health.
- Not wanting to discuss on-line activity and social media use.

Practical strategies to prevent and address the impact of cyberbullying are available at https://www.esafety.gov.au/parents/big-issues/cyberbullying

6.2.2 Sexting

Sexting involves sending or sharing intimate or sexually explicit messages, images, photos or videos. It is essential that students using social media are aware that;

- once an image is shared you lose all control over its future use. It may be copied and saved by others, shared with people the sender does not know, and posted on social media and websites.

- images can be extremely difficult to remove from the internet and the consequences can follow a young person into adulthood.
- sometimes when a relationship breaks down there can be an intent to humiliate an ex-partner or friend. This occurs more frequently than young people may think and is referred to as 'image-based abuse'.
- it is illegal to ask for, access, possess, create or share a sexualised image of children and young people under 18 - even if this occurs between consenting young people. The consequence of this may be a permanent criminal record and registration as a sex offender.

Practical strategies to minimise the risks of sexting, as well as how to respond to children and young people who have sent, received or shared an image are available at https://www.esafety.gov.au/parents/big-issues/sending-nudes-sexting

6.2.3 Unwanted contact and on-line grooming

Unwanted on-line contact is defined as anything that is unpleasant, upsetting or may lead into a situation where someone becomes unsafe. It includes contact with people who are completely unknown, known only on-line, or are known in the real word.

On-line grooming is the most dangerous category type of unwanted contact. It involves adults or young people using the internet (commonly via social media platforms) in a predatory manner to lower a child or young person's inhibitions or trick, pressure or force a child or young person to do something sexual, either over the internet or in person. For adults, on-line grooming is against the law, even if they never meet the child or young person in real life.

Perpetrators of on-line grooming may;

- pretend to be a child or young person themselves.
- request photos or videos.
- request to meet face to face.
- make a child or young person feel special.
- ask where the child or young person lives or for their phone number.
- find things in common with the child or young person.
- offer gifts or favours (e.g. on-line game credits or money)
- persistently seek out the child or young person.
- ask if the child or young person is alone.
- make threats or manipulate the child or young person to do things the perpetrator wants.

Practical strategies to protect students from unwanted contact and on-line grooming include

- ensuring that the highest privacy settings for social media sites are used

- only using a first name or nickname in on-line chat, and to never disclose full name, phone number, address or school.

Further information and strategies are available at
https://www.esafety.gov.au/parents/big-issues/unwanted-contact

6.2.4   Reporting suspected or known cyberbullying, sexting or on-line grooming

As a Child Safe organisation, Berry Street and the Berry Street School has zero tolerance for child maltreatment or abuse and zero tolerance for any Berry Street person failing to report suspected maltreatment or abuse.

Child maltreatment or abuse cannot remain hidden and must be reported in line with Child Safe Standards, the Victorian Reportable Conduct Scheme, DHHS CIMS and the law. Depending on the circumstance and age of the perpetrator or alleged perpetrator, this may include any combination of;

- Immediate notification to the Campus Assistant Principal or the School Principal
- Student support group meeting to introduce targeted support
- If the content is explicit, pornographic or exploitative of students, contacting the eSafety Commission and making a report https://www.esafety.gov.au/report
- Reporting via ERIN
- Reporting to DHHS Child Protection as a mandatory reporting requirement
- Reporting to Victoria Police

Please also refer to Berry Street's *Responding to Child Maltreatment Procedure*.

It is essential that breaches of privacy or on-line abuse does not remain hidden. Students must be supported to contact a teacher, parent, guardian or carer for support as soon as possible.

6.3   Use of social media for school communication

The Berry Street School uses the *Engage* School Management System to communicate with students, parents, guardians and carers, and to administer learning and support.

The Engage 'Parent Portal' will be used as the default communication channel for parents, guardians and carers. Where parents, guardians or carers do not have access to a device the School must select a method that balances practicality with the inherent risks of using social media applications, including permanency of the communication in the public domain and third-party hacking. Given the privacy risks associated with communication via social media, the following protocols must be followed;

- treat every interaction as a permanent record, that may exist on the internet forever;
    o minimise the quantity and sensitivity of information that is communicated (e.g. use the student's initials or first initial).

o don't discuss or disclose personal information, instead make a time for an appointment or a phone call.

- don't disclose the School's location, or references to Berry Street.
- always updating apps and software when prompted to do so via push notifications. Nearly all updates involve security patches that close newly discovered holes in application software.
- ensure that the app being used cannot be opened without a password and/or identifiable information cannot be accessed without a password.
- using strong passwords that use a combination of upper-case and lower-case letters, numbers and punctuation.
- document relevant information communicated and then where possible delete chat threads on the app.
- if you wish to deploy an app or social media channel to connect with a client (or school or community group on behalf of a client) and it is not already in use at Berry Street, please send the request to: clientsystemssupport@berrystreet.org.au

As a general rule, the same standards for communication and interaction that exist in the school, extend to social media.

6.4 Berry Street's corporate social media channels

Social media is used as a tool for Berry Street to connect and communicate with the broader community, including donors, sponsors, employees, volunteers and carers. These corporate channels, include;

- Facebook
- Twitter
- Instagram
- LinkedIn
- YouTube

Only designated employees within the Strategic Engagement team are authorised to establish social media profiles or accounts on behalf of Berry Street, post content on behalf of Berry Street on social media or use social media to conduct Berry Street business.

6.5 Information security

The *Berry Street Information Security Policy* and *Berry Street Information Acceptable Use Policy* provide clear and consistent requirements regarding the protection of Berry Street information assets. All activity on Berry Street devices, information systems and facilities is monitored for policy non-compliance . Staff shall have no expectation of privacy relating to their use of the internet including browsing, email, instant messaging and social media.

6.6 Authorities and accountabilities

6.6.1 The Berry Street School Community

Berry Street requires that all students, teachers and staff understand and follow this policy.

6.6.2 Berry Street School Principal

It is the responsibility of the Principal to ensure that students, teachers and staff are aware of their obligations and responsibilities as outlined in the policy. The Principal will also regularly review this policy and ensure it reflects the needs of the school community.

6.6.3 Executive Director, People and Culture

Ensuring all teachers and School staff (full time, part time, permanent and casual) and volunteers are provided with access to a copy of this policy prior to or at the commencement of their employment.

6.6.4 Berry Street Privacy Officer

It is the responsibility of the Berry Street Privacy Officer to monitor and mitigate privacy risk created through the use of social media.

7 Supporting Documents and References

7.1 Related Berry Street documents

- Berry Street Reporting Child Maltreatment Procedure
- Berry Street Responding to Reports of Child Maltreatment Procedure
- Berry Street Code of Conduct
- Berry Street Client Information Privacy Policy
- Berry Street Information Security Policy
- Berry Street Information Security Acceptable Use Policy
- Berry Street Personal Use of Social Media Policy
- Berry Street Social Media and eSafety within Service Delivery Policy
- Berry Street School Privacy Policy
- Berry Street School Child Safety and Wellbeing Policy
- Berry Street School Student and Family Code of Conduct
- Berry Street School Anti-Bullying Policy

7.2 Other relevant documentation

The following provides an overview of key standards and legislation that apply to the management of Social Media use and on-line environments at Berry Street.

- Enhancing On-line Safety Act (2005)
- Privacy Act 1998 (Cwth) – incorporating the Australian Privacy Principles and the Notifiable Data Breaches Scheme

- Privacy and Data Protection Act 2014 (Vic) – incorporating the Information Privacy Principles and the Victorian Data Security Framework
- Victorian Child Safe Standards 2022
- National Principles for Child Safe Organisations
- Ministerial Order 1359

8   Version control

Version Number	1.1
Approved by:	Berry Street Board
Approved date:	12/12/2023
Review date:	12/12/2026
Process Owner:	School Principal
Executive Responsible:	Executive Director – Statewide Services
External publication:	Yes Policies | Berry Street School
Plain English version:	Yes
Version notes:	
Version 1.0	New Policy
Version 1.1	Update format and seek board approval

If you have any queries in relation to this policy, please contact the School on 9429 4266.