

Policy Statement - Social Media & Information Technology Acceptable Use

1 Policy Statement

- 1.1 To guarantee that staff are aware of the potential risks of social media and what is public or private, personal or professional is respected and adhered to.
- 1.2 To encourage teachers, students and staff to use social networking to enhance the classroom experience, connect with others, share educational resources, create and curate educational content.
- 1.3 To protect all students from inappropriate online conduct / contact from other students and staff including possible abusive behaviour such harassment, trolling and grooming.

2 Introduction

- 2.1 BLCI recognises that access to technology in school gives students and staff greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.
- 2.2 To that end, we provide access to technologies for student and staff use. This Acceptable Use Policy outlines the guidelines and behaviours that users are expected to follow when using school technologies or when using personally owned devices on the school campus.
- 2.3 The network is intended for educational purposes.

All activity over the network or using technologies may be monitored and retained.

Students are expected to follow the same rules for good behaviour and respectful conduct online as offline.

Misuse of school resources can result in disciplinary action.

We make a reasonable effort to ensure students' safety and security online but will not be held accountable for any harm or damages that result from misuse of school technologies.

Users of the network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

3 Technologies Covered

- 3.1 BLCI may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, BLCI will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

4 Usage Policies

- 4.1 All technologies provided by BLCI are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

5 Web Access

- 5.1 BLCI provides its users with access to the Internet, including web sites, resources, content, and online tools. Web browsing may be monitored, and web activity records may be retained indefinitely. Users are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert an IT staff member or submit the site for review.

6 E-mail

- 6.1 BLCI may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the company policy. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

7 Social / Collaborative Content

- 7.1 Recognizing that collaboration is essential to education, BLCI may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally identifying information online.

8 Contact between staff and students under 18:

- 8.1 Staff must not establish or seek to establish social contact with under 18s/pupils before, during or after the course.

Staff must not give personal email addresses or phone numbers to students under 18.

Staff must not communicate via email, text, phone, social networking sites, blogs, web pages or messaging services with under 18s.

A professional attitude must be always maintained, both in and out of school

Staff must be aware that their personal web profiles on social media can be viewed by anyone and therefore should be especially cautious about their public web profiles and privacy settings

- 8.2 Any use of social media by staff and students must:

Staff must only use the school e-mail systems for any electronic contact with a pupil before, during or after a course.

In any electronic contact with pupils' staff must pay particular attention to use neutral language that will not be misconstrued.

Any use of social network sites with under 18s is forbidden. Any staff wishing to set up a Facebook page for students must ensure that there are no under 18s involved

9 Mobile Devices Policy

- 9.1 BLCI may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices, including use of the school network, may be monitored.

10 Personally Owned Devices

- 10.1 Students may use personally-owned devices (including laptops, tablets, smartphones, and cell phones) at any time during school hours – unless such use interferes with the delivery of instruction by a teacher or staff or creates a disturbance in the educational environment. Any misuse of personally owned devices may result in disciplinary action. Therefore, proper netiquette and adherence to the acceptable use policy should always be used. In some cases, a separate network may be provided for personally owned devices.

11 Security

- 11.1 Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

12 Downloads

- 12.1 Users should not download or attempt to download or run .exe programs, additional toolbars or web browser plug-ins/add-ons over the school network or onto school resources without express permission from IT staff. You may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.

13 Netiquette

- 13.1 Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- 13.2 Users should also recognise that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.
- 13.3 Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there – and can sometimes be shared and spread in ways you never intended.

14 Plagiarism

- 14.1 Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images, from the Internet.

- 14.2 Users should not take credit for things they didn't create themselves or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

15 Personal Safety

- 15.1 If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of your line manager immediately.

Users should never share personal information, including phone number, address, social security number, birthday, or financial information.

Users should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others.

Users should never agree to meet someone they meet online in real life.

16 Cyberbullying

- 16.1 Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

17 Examples of Acceptable Use

Use of school technologies for school-related activities and research.

Following the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.

Treating school resources carefully, and alert staff if there is any problem with their operation.

Encouraging positive, constructive discussion if allowed to use communicative or collaborative technologies.

Alerting a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.

Using school technologies at appropriate times, in approved places, for educational pursuits only.

Citing sources when using online sites and resources for research; ensure there is no copyright infringement.

Recognising that use of school technologies is a privilege and treat it as such.

Being cautious to protect the safety of myself and others.

Helping to protect the security of school resources. This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

18 Examples of Unacceptable Use

Using school technologies in a way that could be personally or physically harmful

Searching inappropriate images or content.

Engaging in cyberbullying, harassment, or disrespectful conduct toward staff or students.

Trying to find ways to circumvent the school's safety measures and filtering tools.

Using school technologies to send spam or chain mail.

Plagiarising content I find online.

Posting personally identifying information, about myself or others.

Agreeing to meet someone I meet online in real life.

Using language online that would be unacceptable in the classroom.

Using school technologies for illegal activities or to pursue information on such activities.

Attempting to hack or access sites, servers, accounts, or content that isn't intended for my use. This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

19 Limitation of Liability

- 19.1 BLCI will not be responsible for damage or harm to persons, files, data, or hardware. While BLCI employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. BLCI will not be responsible, financially or otherwise, for unauthorised transactions conducted over the school network.

20 Violations of this policy

- 20.1 Violations of this policy may have disciplinary repercussions, including:
- Suspension of network, technology, or computer privileges in extreme cases
 - Notification to parents in most cases
 - Detention or suspension from school and school-related activities
 - Legal action and/or prosecution

21 Guidelines:

21.1 Use good judgment

We expect you to use good judgment in all situations.

You must know and follow the school's code of conduct as set out in the Safeguarding Policy and our Data Protection Policy.

Regardless of your privacy settings, assume that all the information you have shared on your social network is public information.

21.2 Be respectful

Always treat others in a respectful, positive and considerate manner.

21.3 Be responsible and ethical

Even though you are approved to represent the school, unless you are specifically authorised to speak on behalf of the school as a spokesperson, you should state that the views expressed in your postings, etc. are your own. Stick with discussing school-related matters that are within your area of responsibility.

Be open about your affiliation with the school and the role/position you hold.

21.4 Be a good listener

Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly and to share feedback.

Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback, etc.

Always be doing at least as much listening and responding as you do “talking.” Don’t share the following:

22 Confidential information

22.1 Do not publish, post or release information that is considered confidential or not public. If it seems confidential, it probably is. Online “conversations” are never private. Do not use your birth date, address, and cell phone number on any public website. Private and personal information:

To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules or situations.

Never give out or transmit personal information of students, parents, or co-workers

Don’t take information you may receive through social networking (such as e-mail addresses, customer names or telephone numbers) and assume it’s the most up-to-date or correct.

Always respect the privacy of the school community members.

22.2 Please be cautious with respect to Images:

Respect brand, trademark, copyright information and/or images of the school (if applicable).

You may use photos and video (products, etc.) that are available on the school’s website.

Do not post pictures of others (co-workers, etc.) without their permission.

23 Other sites

A significant part of the interaction on blogs, Twitter, Facebook and other social networks involves passing on interesting content or linking to helpful resources. However, the school is ultimately responsible for any content that is shared. Don’t blindly repost a link without looking at the content first.

Pay attention to the security warnings that pop up on your computer before clicking on unfamiliar links. They serve a purpose and protect you and the school.

When using Twitter, Facebook and other tools, be sure to follow their printed terms and conditions. And if you don't get it right:

Correct any mistake you make immediately and make it clear what you've done to fix it.

Apologise for the mistake if the situation warrants it.

If it's a major mistake (e.g., exposing private information or reporting confidential information), please let someone know immediately so the school can take the proper steps to help minimise the impact it may have.

GF/NR/LK