Social Media Policy

Policy Review & Update Process			
Member(s) of SLT responsible for update		Jonathan Poole	
Sub-Committee responsible for review		Marketing	
ISBA template policy?		No	
Last Updated	**September 2024**	Updated by	**JP**
Last review	**September 2022**	Next review	**September 2026**

Contents

Policy Statement

To ensure clarity of use and guidance for staff, students and all users regarding the use of social media and networking applications, the impact on work and the staff code of conduct and all associated matters.

The policy is designed to protect individual members of staff, students and all users.

This policy applies to the use of social media for both business and personal purposes, whether during School/working hours or otherwise. The policy applies regardless of whether the social media is accessed using school IT facilities and equipment or equipment belonging to members of staff or any other IT equipment.

Rationale

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new, relevant and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with duties to the School, the community, our legal responsibilities and our reputation.

The School use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff across the Pre-Prep and Prep departments.

The purpose of the policy is to:

• Safeguard all students and promote wellbeing;
• Ensure users are not exposed to risk as a result of their actions;
• Use social media in a respectful and productive way which respects all parties involved;
• Ensure that the reputation of Bickley Park School (the School), its staff and governors is protected and that stakeholders understand their ambassadorial role with regard to the School;
• Protect the School from legal risks;
• Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the School.

Definition and Scope of Social Media

The School defines social media as "any method of communication in cyberspace." This includes written or verbal mobile phone conversations, email communication via computers, phones, iPads and similar tablets, and written or verbal conversations via computer transmission. Social networking sites and tools include, but are not limited to, Facebook, WhatsApp, Google Plus, MySpace, Bebo, Friendster, video and photo sharing websites like Flickr, YouTube and Instagram. It also includes micro-blogging sites such as X (Twitter), weblogs, including organizational blogs, personal blogs or blogs hosted by traditional media

publications, forums and discussion boards such as Yahoo! Groups or Google Groups, online encyclopaedias such as Wikipedia, and any other web sites which allow individual users or organisations to use simple publishing tools.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All members of the School should bear in mind that information they share through social networking applications, even if they are on private spaces, may be subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Child Protection and Safeguarding Policy, E-Safety Policy, Equal Opportunities Policy, Behaviour Policy, Taking, Storing and Using Images of Children Policy, Camera and Mobile Phones Policy.

The Malicious Communications Act 1988 Chapter 2 and Section 127 of the Communications Act 2003 apply to all social media interaction by pupils, staff and parents of the School.

Within this policy there is a distinction between use of School sanctioned social media for professional educational purposes, and personal use of social media.

Use of social media in practice for Staff

Use of social media in practice for personal and professional use

4.1. Staff must not have 1:1 communication, including direct messaging (DM), with students through any social media, apart from via school email accounts, and school mobile / tablet devices for messaging.

4.2. Staff should not request or accept any current student of the School of any age or any ex-student of the School under the age of 18 as a friend, follower, subscriber or similar on any personal social media account unless they are the parent of the pupil or a close family member.

4.3. It is advisable that staff do not have contact with past pupils (above school age). Staff may remain in communication with past pupils via a school email account or the School social media accounts.

4.4. Any communication received from current pupils on any personal social media sites must be reported immediately to the Designated Safeguarding Lead (DSL).

4.5. If any member of staff is aware of any inappropriate communications involving any student in any social media, these must immediately be reported to the Designated Safeguarding Lead (DSL)

4.6. Members of staff must ensure that, wherever possible, and where the social media site allows, their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives or follow them on their personal accounts.

4.7.   All email communication between staff and students of the School on school business must be made from an official school email account (any deviation from this in an emergency must at once be reported to the line manager). Staff should not use personal email accounts or personal mobile phones to make contact with students of the School, nor should any such contact be accepted, except in circumstances such as school trips or away matches that have been given prior approval by the Head. Prior approval may also be given by the Head or staff to communicate professionally with students on School premises for safety reasons.

4.8.   Staff should not post or publish on the internet or on any social networking site, any reference to the School, their colleagues, parents or pupils or discuss pupils or colleagues or criticise the School or staff. Staff may like, share or make appropriate comment in response to the School's official social media accounts, in accordance with 4.11.

4.9.   Staff must not post images on any social media account that includes pupils, unless sharing posts made from the School's official social media account.

4.10.   Staff are instructed to consider the reputation of the School in any posts or comments related to the School on any social media accounts. Reputational breaches by staff are dealt with via the Disciplinary Policy.

School-sanctioned use of social media

There are many legitimate uses of social media within the curriculum, and to support student learning and to share news with the wider Bickley Park School community. For example, the School and sub-departments of the School have official Twitter, Instagram and Facebook accounts. There are also many possibilities for using social media to enhance and develop students' learning and to keep the Bickley Park School Community and our supporters in touch with the School.

When using school social media accounts for School purposes, the following practices must be observed:

5.1.   Staff should set up a distinct and dedicated social media site or account. This should be entirely separate from any personal social media accounts held by that member of staff, and should be linked to an official school email account. Social media accounts must have a link to the Social Media Policy, have official Bickley Park School branding by the Marketing Department and state that it is an 'Official Bickley Park School Approved Site'

5.2.   The social media account must be approved by the Head and/or Marketing Manager prior to publication and the identity of the site and password must be shared with the Marketing Department.

5.3.   The content of any School-sanctioned social media site should be solely professional and should reflect well on the School. Content should be approved by the Headmaster and/or Marketing Manager prior to publication.

5.4.   Staff must not publish photographs of students without the written consent of parents / carers. For all children standard practice is to publish only the first name of the child, unless permission has been given by parents for the full name to be used. School sanctioned social media sites must use only images of children in suitable clothing.

5.5.   Staff must take into account the Child Protection and Safeguarding Policy and the Staff Code of Conduct when making any posts on school social media accounts.

5.6.   Staff must ensure that any links to external sites from the accounts are appropriate and safe; if they are shared, these must be verified as reputable sites. Only appropriate hashtags should ever be used.

5.7.   Any inappropriate comments on, or abuse of, school-sanctioned social media should immediately be removed and reported to Head, DSL, Network Manager and the Marketing. It is the responsibility of everyone using the site and social media in general to report abuse immediately.

5.8.   Staff should not engage with any direct messaging of students through social media where the message is not public.

5.9.   All school sanctioned social media accounts created for School purposes should include a link in the About or Info page to the E-Safety and Computer Usage Policy on the School website. This will indicate that the account is officially sanctioned by the School.

Social Media Policy – Guidance and Advice for Staff

Most common social networking sites are inherently insecure places to have discussions which contain any sensitive information. Privacy laws can be violated and the reputation of our school can be damaged if the public sees a discussion of any sensitive information taking place on social networking. Staff should be aware that these types of cases can result in disciplinary action.

Proprietary Information

Staff may not share information which is confidential and proprietary about the School. This includes information about services, programmes, financial, strategy, and any other internal confidential, proprietary, or sensitive workplace information that has not been publicly released by the School. These are given as examples only and do not cover the range of what the School considers confidential and proprietary. If staff have any questions about whether information is proprietary, they must speak to their Line Manager or SLT member before releasing it. Staff must also be aware of the points made within their employment contract when they joined the School.

The School's logo and mascots may not be used without explicit permission in writing from the Marketing Department; the School owns the rights to all logos, mascots, mottos and phraseology and their usage.

Workplace Privacy

The School respects staff member rights to privacy and to express themselves. However, the School and staff members must also respect, and diligently protect, the privacy of fellow staff members, students, parents, and others. Privacy and confidentiality must be maintained in every possible way.

It is both inappropriate and illegal to discuss pupil or family related information via social networking and public social media, texting, or online unless it is an approved medium and for a school related purpose. The School must have written permission from the legal guardian for that particular information to be divulged.

Staff are advised to be extremely cautious in conversations with other staff, parents and volunteers in social networking, on the basis that privacy laws can be violated even if a person's name is not shared.

The School will honour the privacy rights of current and past employees, current and past students and their families, and anyone else associated with the School, by seeking permission before writing about or displaying internal school happenings which might be considered to be a breach of their privacy and confidentiality.

Privacy and Security Settings

The School recommends staff use security and privacy settings provided by social networking sites. Regardless of privacy settings, staff are advised to be respectful and responsible in all activity if it in any way involves or references the School, job, or those staff work with.

Staff must understand that on-line content is difficult, if not impossible to retract once posted or sent and to be aware of the long memory of cyberspace.

Staff and students are reminded that privacy settings are overridden if they watch or look at a site containing a warning that watching or looking will give access to the rest of the site.

Blogging and Websites

If staff or pupils are developing a website or writing a blog that will mention the School and/or our Common Room, staff, Governors, students, parents and volunteers, they MUST get permission first before writing anything, and advise the Headmaster they are intending to do this. The Head may choose to visit from time to time.

It is important that staff make appropriate decisions about work-related blogging and the content of blogs, personal websites, postings on wikis and other interactive sites. Staff are advised to use caution with postings on video or picture-sharing sites, or in comments made elsewhere on the public internet and in responding to comments from posters either publicly or via email. If staff are assisting students to develop a website or blog, this must first be approved by the Head/SLT member and the Head /SLT member must be given password access.

All students must understand and sign the ICT Acceptable Use Policy prior to engaging in cyberspace in the classroom.

Disclaimer

When utilising social networking, if staff choose to provide any thoughts or advice to others and it is known that you are a part of the School, it is wise to include a disclaimer such as:

"I am an employee of Bickley Park School and the views expressed here are mine alone and do not necessarily represent that of the School."

This does not eliminate the possibility of bringing the School into disrepute.

Legal Liability

Staff should recognise that there is the possibility of being legally liable for something inappropriate which is shared online. Some individuals have been sued by other employees, parents, other individuals or a company which viewed their commentary, content, or images as defamatory, pornographic, proprietary, harassing or breach of copyright.

The Media

If a member of the media or non-traditional online media (including bloggers) contacts a member of staff about the business of the School (e.g., programmes, services, students, parents, clubs, policies, practices, or additional business information of any kind), the individual must contact the Marketing Department prior to responding.

Use of Social Media in Practice for Students

7.1. Students must not access any social media that is for adults only.

7.2. Anonymous must not be accessed as there is a high risk that inappropriate comments can be exchanged, causing distress or endangerment.

7.3. Bad, including offensive, explicit or abusive, language and inappropriate pictures must never be included in messages.

7.4. All messages should be positive and not include anything that could be upsetting or defamatory towards others or the School.

7.5. Students must take responsibility for keeping details of their accounts private, using full privacy settings and logging off properly and not allowing others to use their accounts.

7.6. Students must report anything offensive or upsetting that they see online to the appropriate bodies, either by using the "report abuse" tabs or by speaking to their parents or a member of staff.

7.7. It is a serious offence to use another person's account, or to create an account in another person's name without their consent.

7.8. Students should not regard anything posted online as private and should remember that harassment, defamatory attitudes and racism are just some of issues which could lead to prosecution.

7.9.   An individual's "Digital Footprint" is becoming increasingly significant when it comes to job and university applications. If unfortunate decisions are made, it will be extremely difficult, perhaps impossible, to eliminate the evidence.

7.10.   If students see inappropriate postings by other students, they must inform the school so that steps can be taken to avoid possible repercussions.

7.11.   The Malicious Communications Act 1988 Chapter 2 and Section 127 of the Communications Act 2003 apply to all social media interaction by Pupils, Staff and Parents of the School.

7.12.   The attached "Age Restrictions for Social Media Platforms" document is useful for reference. It demonstrates the ages at which children are allowed to access various Social Media platforms, as well as serving as a starting point for discussion about the safe use of Social Media.

Use of Social Media in Practice for Parents

8.1.   Contributions to the School Social Media, such as Twitter, are welcomed.

8.2.   Any concerns or issues about the School, its students or staff should be expressed directly to the School and not be voiced on social media.

8.3.   Parents must obtain permission before posting pictures that contain other parents or their children, unless sharing or liking a post from the School's official social media account.

8.4.   If parents become aware of inappropriate use of social media by their own or other people's children, they should contact the School so that the School can work with the parents to educate young people on safe and appropriate behaviour.

8.5.   If parents become aware of the inappropriate use of social media by other parents or school staff, they should inform the School so that steps can be taken to remedy the situation.

Further Guidance

Further guidance on educating and safeguarding young people online and responding to incidents:

Online safety advice for pupils, parents and teachers:

www.thinkuknow.co.uk

http://www.saferinternet.org.uk/

https://www.internetmatters.org/

Cyberbullying

www.childnet.com/cyberbullying-guidance

Preventing radicalisation

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-

radicalisation