Non-Statutory

Social Media/Networking Policy

Introduction

This policy applies to all school staff, Governors and Volunteers regardless of their employment status. It is to be read in conjunction with the school's Online Safety Policy. This policy does not form part of the terms and conditions of employee's employment with the school and is not intended to have contractual effect. However, it does set out the school's current practices and required standards of conduct and all staff are required to comply with its contents. Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the school's Disciplinary Policy and Procedure.

This Policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

Purpose of This Policy

The school recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media such as Facebook, LinkedIn, Instagram, TikTok, WhatsApp and Wikipedia. However, staff use of social media can pose risks to the school's confidential and proprietary information, its reputation and it can jeopardise compliance with the school's legal obligations.

To minimise these risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate work-related purposes, all school staff are required to comply with the provisions in this policy.

Who is Covered by This Policy?

This policy covers all individuals working within the school, including senior managers, officers, governors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as *Staff* in this policy).

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

Scope and Purpose of This Policy

This policy deals with the use of all forms of social media including but not limited to Facebook, LinkedIn, Instagram, TikTok, WhatsApp and Wikipedia and all other social networking sites and all other internet postings including blogs.

It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or personal equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal.

Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether the school's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with any investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Personnel Responsible for Implementing This Policy

The Co-Headteachers have overall responsibility for the effective operation of this policy but have delegated day-to-day responsibility for its operation to the school IT Network Manager.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Co-Headteachers in liaison with the IT Network Manager.

All senior school staff have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All school staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the IT Network Manager in the first instance.

Questions regarding the content or application of this policy should be directed by email to office@oakgreen.bucks.sch.uk. marked for the attention of the IT Network Manager.

Compliance with Related Policies and Agreements

Social media should never be used in a way that breaches any of the school's other policies. If an internet post would breach any policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

a) Breach the school's Online Safety policy;
b) Breach the school's obligations with respect to the rules of relevant regulatory bodies;
c) Breach any obligations they may have relating to confidentiality;
d) Breach the school's Disciplinary Rules;
e) Defame or disparage the school, its Staff, its pupils or parents, its affiliates, partners, suppliers, vendors or other stakeholders;
f) Harass or bully other Staff in any way or breach our Anti-harassment and bullying policy;
g) Unlawfully discriminate against other Staff or third parties or breach our Equal Opportunities policy;
h) Breach the school's Data Protection policy (for example, never disclose personal information about a colleague online);
i) Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements); and
j) Breach the school's obligations for Keeping Children Safe in Education.

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the school and create legal liability for both the author of the reference and the organisation.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Personal Use of Social Media

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.

Staff should not use a work email address to sign up to any social media. Staff personal social media pages should not make reference to their employment with the school (excluding LinkedIn, where prior permission should be sought from the Co-Headteachers.

Staff must not take photos or posts from social media that belong to the school for their own personal use.

Staff must not befriend any pupils at the school and any such friend requests should be notified to the Network Manger/DSL so that these may be logged.

Staff should not befriend any parents of pupils at the school. In the circumstance where a parent becomes a member of staff and already have parents as “friends” on any social media account they should consider carefully whether these existing social media relationships will cause a conflict of interest with their professional role.

All new staff are reminded of their professional code of conduct in their Online Safety & GDPR induction with support on how to manage such conversations with parents.

Monitoring

The contents of our IT resources and communications systems are the school’s property. Therefore, staff should have no expectation of privacy in any message, files, data, document, telephone conversation, social media post conversation or message or any other kind of information or communications transmitted to, received or printed from or stored or recorded on our electronic information and communications systems.

The school reserves the right to monitor, intercept and review, without further notice, staff members activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that the school’s rules are being complied with and for legitimate business purposes. By your acknowledgement of this policy consent is deemed to have been given to such monitoring and your use of such resources and systems. This might include without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The school may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

All Staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the school.

Educational and Extra-Curricular Use of Social Media

No member of staff will communicate with the media without express permission of the Co-Headteachers.

All members of staff will ensure that any communication with any types of media outlets is in accordance with the guidelines set out in our Media Relations Policy.

Recruitment

The school may use internet searches to perform pre-employment checks on candidates in the course of recruitment. Where the school does this, it will act in accordance with its data protection and equal opportunities obligations.

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

Responsible Use of Social Media

Photographs for use with social media:

Any photos for social media posts including staff, pupils or school buildings may only be taken using school devices. Where any device is used that does not belong to the school this may incur disciplinary action. All photos taken on any device not owned by the school must be deleted immediately from the device once the photos have been uploaded to a device belonging to the school.

Images may only be used in accordance with the Online Safety, Acceptable Use, Mobile Phones, Personal Devices and Imaging Policies.

- Permission to use any photos or video recordings must be gained from parents/carers and in accordance with GDPR.
- If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload pupil pictures online other than via the school owned social media accounts.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

Staff protocol for use of social media:

Where any post is going to be made on the school's own social media the following steps must be taken:

1. Ensure that specific permission from the child's parent/carer has been sought before information is used on social media
2. Ensure that there is no identifying information relating to a child/children in the post - for example, any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work. The school should seek additional consent to include any names when posting on social media.
3. The post must be a positive and relevant post relating to the children, the good work of staff, the school or any achievements.
4. Social media can also be used to issue updates or reminders to parents/guardians
5. The proposed post must be presented to the IT Network Manager for confirmation that the post can 'go live' before it is posted on any social media site.

6. The IT Network Manager will post the information but all staff have responsibility to ensure that the Social Media Policy has been adhered to.
7. Personal information shared/published on social media will be required to be disclosed under a subject access request.

Pupils and Social Media

From Spring 2027, under-16s will no longer be able to use certain social media.

Children will still be able to go online safely, for learning, news, games and staying in touch with friends and family.

16 and 17 year olds will still be able to access social media, but live streaming, and stranger communication including in gaming, will be switched off by default for these ages.

This Policy will be reviewed and any recommendations adopted at that time.

Protecting our business reputation:

Staff must not post disparaging or defamatory statements about:

i. The school;
ii. Current, past or prospective Staff as defined in this policy
iii. Current, past or prospective pupils
iv. Parents, carers or families of (iii)
v. The school's suppliers and services providers; and
vi. Other affiliates and stakeholders.
vii. Current, past or prospective governors

Staff should also avoid social media communications that might be misconstrued in a way that could damage the school's reputation, even indirectly.

If Staff are using social media they should make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than school e-mail address when communicating via social media.

Staff are personally responsible for what they communicate in social media. Staff should be mindful that what they publish might be available to be read by the masses (including the school itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before they post content.

If Staff disclose directly or indirectly their affiliation to the school as a member of Staff whether past, current or prospective, they must also state that their views do not represent those of the school.

Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.

Staff must avoid posting comments about confidential or sensitive school related topics. Even if Staff make it clear that their views on such topics do not represent those of the school, such comments could still damage the school's reputation and incur potential liability.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they have discussed it with his/her Line Manager.

If a member of Staff sees content on social media that disparages or reflects poorly on the school including its Staff, pupils, parents, service providers, stakeholders or governors, they are required to report this in the first instance to the Co-Headteachers without unreasonable delay. All staff are responsible for protecting the school's reputation.

Process for creating new accounts

The school will consider the following points when creating a school social media account:

- Will it enhance the teaching and learning for pupils.
- Will it aid communication with parents/carers.
- Will it showcase the school to the wider community.
- Who is the intended audience.
- How will the account be promoted.
- Who will have access to the account .
- What restrictions will be applied to the account.

Respecting intellectual property and confidential information:

Staff should not do anything to jeopardise school confidential information and intellectual property through the use of social media.

In addition, Staff should avoid misappropriating or infringing the intellectual property of other school's, organisations, companies and individuals, which can create liability for the school as well as the individual author.

Staff must not use the school's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Co-Headteachers.

To protect yourself and the school against liability for copyright infringement, the Staff member should, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Co-Headteachers in the first instance before making the communication.

Respecting colleagues, pupils, parents, clients, service providers and stakeholders:

Staff must not post anything that their colleagues (past and/or current), pupils (prospective and/or current), parents, service provider, stakeholders or governors may find offensive, including discriminatory comments, insults or obscenity.

Staff must not post anything relating to colleagues (past and/or current) or pupils, parents (prospective and/or current) service providers, stakeholders or governors without their advanced written permission.

Monitoring and Review of This Policy

The IT Network Manager together with Co-Headteachers shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice. The Governing Body has responsibility for approving any amendments prior to implementation.

The Co-Headteachers have responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.