



The Crypt School

Social Media Policy

Lead Person:	Deputy Head (Pastoral)
Governing Body Committee:	Pupil Education and Outcomes

1. Social Media

Social Media is used increasingly across society and is recognised as a hugely valuable communication tool. However, the open nature of the internet means that social networking sites can leave professionals (such as teachers and other staff working in education) vulnerable. This policy is intended to protect The Crypt School staff and pupils from potential harm.

In line with our school values, all staff who choose to do so are expected to use social media responsibly, respectfully and with integrity. Pupils must only use social media in line with any government and app age restrictions, and we advise all parents/ carers to closely monitor pupil's activity online via mobile phones and iPads, including any messages or disappearing messages where possible.

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 and pupils at the School. The purpose of the policy is to:

- Safeguard all pupils and promote wellbeing;
- Ensure users are not exposed to risk as a result of their actions;

- Encourage members of the community to use social media in a respectful, positive and productive way;
- Ensure that the reputation of The Crypt 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.

2. Policy Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.
- Defines the monitoring of public social media activity pertaining to the school.

The school respects privacy and understands that staff and pupils may use social media in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy. Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy. However, school iPads and laptops are subject to Network Monitoring and must not be used for personal social media activity.

Staff may use social media to communicate with pupils via a school social media account only through posting content to all followers. There must be no private messages or groups or favourites (or similar) linked to any school social media accounts. Staff, including volunteers, must not send or respond to messages or comments from students on school social media accounts. If further dialogue is needed around any social media post, school email must be used.

Any content created by staff (for example for YouTube or a podcast) must not bring the school into disrepute, nor should it name or refer to the school unless prior approval has been gained from the Headmaster.

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.

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 our 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 cooperate with our investigation, which may involve handing over relevant passwords and login details so far as this is consistent with the right of an individual to private and family life. Staff may be required to remove internet postings which are deemed to constitute a breach of this policy.

3. Implementation of the policy

The Headmaster has overall responsibility for the effective operation of this policy, but has delegated day to day responsibility for its operation to the Network Manager. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risk also lies with the IT Network Manager, working alongside Deputy Headteacher (Pastoral).

All Heads of Departments have a specific responsibility for operating within the boundaries of this policy, ensuring that all their departmental staff understand the standards of behaviour expected of them and if necessary enforcing this policy by taking action when behaviour falls below its requirements.

All staff are responsible for their own compliance with this policy and ensuring that it is consistently applied to protect the privacy, confidentiality, reputation and interests of the School. Any misuse of social media should be reported to the Network Manager who will liaise with the Deputy Headteacher (Pastoral) at the earliest opportunity. Questions regarding the content or application of this policy should be directed to the Network Manager.

4. Relationship with other School policies

If an internet post would breach any of our policies in person it will also breach them online. For example, staff are prohibited from using social media to:

- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach our Disciplinary Rules;
- defame or disparage the School or our affiliates, parents, staff, pupils, business partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way or breach our Anti-bullying and hate policy;

- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities policy;
- breach our Data Protection policy (for example, never disclose personal information about a colleague, pupil or parent online). Staff are still obligated not to disclose information they have had access to during employment at the School after they have ceased to be in its employ;
- 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).

Information shared online can be permanent and so staff must be cautious about what they say and what they display as it can be harder to retract. If in any doubt as to how to meet this responsibility at any time, please speak to your line manager. Staff must also be aware of the particular risks to internet security that social media presents and must take any extra measures necessary not allow any of their actions on social media sites to create vulnerability to any School systems.

5. Responsible use of social media

Staff

Staff must be aware that their role comes with particular responsibilities and they must adhere to the School's strict approach to social media and act in line with our school values.

Staff must:

- be kind and respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see.
- **staff members are responsible for setting, and regularly checking the privacy levels of their personal social media sites** as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy.
- keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.
- obtain the prior written approval of the Headmaster, to the wording of any personal profile which they intend to create where the School is named or mentioned on any social networking site except LinkedIn;
- seek approval from the Headmaster before they speak about or make any comments on behalf of the School on the internet or through any social networking site;
- Report to their Head of Department or Line Manager immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School. **If the information seen concerns the welfare of a child, this must be reported immediately to the Deputy Headteacher (Pastoral) in person or via safeguarding@crypt.gloucs.sch.uk;**
- Immediately remove any internet postings which are deemed by the School to constitute a

breach of this or any other School policy;

- Consider whether a particular posting puts their credibility or effectiveness as a teacher or member of school staff at risk;
- Staff members must not identify themselves as employees of The Crypt School in their personal web space apart from professional websites such as LinkedIn. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members.

Staff must not:

- provide references for other individuals on social or professional networking sites, as such references whether positive or negative can be attributed to the school and create legal liability for both the author of the reference and the school;
- post or publish, on the internet or on any social networking site, any negative reference to the School, their colleagues, parents or pupils;
- use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations;
- discuss pupils or colleagues or publicly criticise the School or staff;
- post images that include pupils unless it is on official School social media accounts and then only if the parent/guardian of the student has consented for their child's image to be shared in this way.
- have social media contact with any pupil's family members (parents/carers) unless they were known to you prior to the child joining the school. This is inline with the teachers' unions which say that teachers should never under any circumstances accept social media friend requests from parents of a pupil;
- accept as friends/ contacts on social or professional networking sites (including LinkedIn) current pupils, ex pupils who are not adults (over 18), or other children or young people, where there is a relationship developed as part of their professional role, e.g. music teacher, sports coach (this is not intended to mean family or relations);
- use social networking sites as part of the educational process e.g. as a way of reminding pupils about essay titles and deadlines (unless, for example, sharing details about an external academic competition).

When a staff member leaves and they have either had access to one or more school owned social media platforms (e.g. Departmental Twitter/X or Instagram accounts) they relinquish access to and responsibility for the account and must not post any further items on that account. Passwords will be changed by the Network Manager and responsibility given to another member of the department;

Staff members must not make contact through any personal ICT or social medium with any pupil, unless the pupil* is your own family member OR an existing close family friend (e.g. your godchild). The Crypt School does not expect staff members to discontinue contact with their own family members or significant family friends via personal social media if the School starts providing support for them. However, staff are required to inform their line manager of their relationship/association with any new or existing pupil so that any potential conflicts of interest or other potential issues can be discussed and avoided.

** 'pupil' is defined as any young person aged 18 or under. Or, any young person who has been a pupil with The Crypt School (or pupil staff have met in another school in their professional capacity) who is no longer in a school or a sixth form up until they reach the age of 18.*

Social Media guidance for staff

1. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
2. Be careful about tagging other staff members in images or posts
3. Do not share anything publicly that you would not be just as happy showing your pupils
4. **Do not** use social media sites during school contact time
5. **Do not** make comments about your job, your colleagues, our school or your pupils online
6. **Do not** associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
7. **Do not** link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
8. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)
9. While some people advocate changing your display name (e.g. to first name and middle name) you should consider this carefully as it can cause problems with proving ownership of your social media account e.g. Facebook
10. Be aware that just because you do not have a profile, it does not mean you do not have a presence on social media. If your friends have accounts, they may have shared photos featuring you that you are not aware of. Talk to your friends and family about posting photos with you in them and how this can impact your work.

Check your privacy settings:

- On sites such as Facebook, change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you have shared and look at your pictures if they're friends with anybody on your contacts list
 - **Do not** forget to check your old posts and photos and consider if they are appropriate to be shared online
 - The public may still be able to see posts **you have** 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
 - Google /web search your name to see what information about you is visible to the public
 - Remember that some information is always public; your display name, for example on Facebook or Instagram your profile picture, cover photo. Your handle, country, age range and gender may also be visible.

What to do if... a pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile.
- Notify the Deputy Head (Safeguarding, Inclusion and Wellbeing) or any Deputy Designated Safeguarding Lead about what is happening
 - Check your privacy settings again, and consider changing your display name or profile picture.
 - If the pupil asks you about the friend request in person, tell them that **you are** not allowed to accept friend requests from pupils and that if they persist, you will have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages and pass to the DSL.

....a parent adds you on social media

- Do not accept the request
- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- In ignoring the message, consider drafting a stock response to send via school email to let the parent know that you're doing so and seek advice from the Deputy Head (Safeguarding, Inclusion and Wellbeing) if required.

....you're being harassed on social media, or somebody is spreading something offensive about you

- Do not retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
 - Report the material to the relevant social media app/ site and ask them to remove it
 - If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
 - If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
 - If the comments are racist, sexist, of a sexual nature, constitute a hate crime or otherwise prejudicial, you or a senior leader should consider contacting the police

Pupils

- Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.
- The Personal Development (PSHE) curriculum teaches pupils to use social media responsibly, risks and benefits of AI and how to stay safe online. This is reinforced through assemblies and form resources during Online Safety Week.
- Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the Behaviour Policy.

- Pupils should not ‘friend request’ or ‘follow’ either current or former staff on social media accounts and are asked not to search the digital footprint of any staff, eg: Google search. Breaches of this will be resolved by the use of the Behaviour Policy.

- If any pupils are worried about anything in relation to AI or the online world (or worried about anything at all) they can speak to a Pastoral Support Worker in our calm and quiet Pastoral Room (and pastoral offices in Sixth Form) any time.

Parents/Carers

- The School educates parents and carers about the safe and positive use of social media through letters, newsletters and via the school website.
- Parents/carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school’s complaints procedures.
- Parents and carers are also encouraged to talk to their children in an age appropriate way about what they choose to share publicly online, and their right to say no if they are invited to feature in photographs that others may post or share.
- Additionally, if parents or carers have any technical questions or would like an image of their child taken down from our school website or social media, they can contact ITsupport@crypt.gloucs.sch.uk.

6. Managing school social media accounts

The Crypt School embraces social media as a modern communication tool with all members of The Crypt community and potentially wider society. Staff can post on the School’s main social media accounts by emailing details to IT Support (who update marketing outlets for the school). Account managers (eg: Heads of Department for a subject based account), must adhere to the following:

Do:

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have consent to share any images of pupils or staff
- Think before responding to comments and, when in doubt, get a second opinion from the Deputy Headteacher (Pastoral) or another member of SLT
- Consider turning off tagging people in images where possible
- Consider the appropriateness of content for any audience of school accounts
- Try to make posts engaging, informative and professional

Do not:

- **Do not** make comments, post content or link to materials that will bring the school into

disrepute

- **Do not** publish confidential or commercially sensitive material
- **Do not** breach copyright, data protection or other relevant legislation
- **Do not** link to, embed or add potentially inappropriate content
- **Do not** post derogatory, defamatory, offensive, harassing or discriminatory content
- **Do not** use social media to air internal grievances
- Do not express personal or political views

Department, Club and Society Social Media Accounts

Clubs and societies may set up and operate their own BlueSky, or Instagram accounts. If a member of staff would like to set-up a BlueSky, or Instagram account for their department, they must first seek permission from the relevant Head of Department and then the Headmaster. If a member of staff would like to set up an account using a social media platform other than BlueSky, or Instagram, they must seek permission from the relevant Head of Department and the Headmaster.

Passwords should be strong, and should be sent to the Network Manager to be stored securely, in order that all School social media accounts are accessible. Pupils must not have password access to, or operate, department social media accounts.

Branding and Presentation

Staff should be aware that all School social media accounts and posts represent the School, and must be consistent with our aims and values. Department accounts must use the correct version of the School crest, and all other images or video clips should be of good quality and reflect the School's brand and high standards - please consult the Headmaster if guidance is required.

Inappropriate Content and Use

School social media accounts must not be used to post, share or spread inappropriate content, or to take part in any activities that may bring the School into disrepute. When sharing a third-party news article, blog post or other piece of content on School social media accounts, staff must always review the content and source thoroughly before posting. Staff must not post or share confidential or sensitive information on social media. (Also see Acceptable Use Policy and Staff Code of Conduct)

Photo Permissions for Pupils

Photo permissions must be checked for all students appearing in pictures posted on the School website, and on School, department, club or society social media accounts. Staff must not post pictures of pupils for whom we do not have permission to do so. Permissions can be checked via Bromcom and / or the Data Administrator.

Pupil-run Social Media Accounts

Pupils running a social media account associated with the School, for example a School society or club, must give password access to their supervising member of staff, who must

also pass the details to the Network Manager. Before the pupil leaves, control must be handed to another person. This includes changing the email address and phone number associated with that account. As stated above, pupils must not have password access to, or operate, department social media accounts. The supervising member of staff is responsible for regularly monitoring the account, ensuring that branding and use of the school crest is correct. The member of staff should ensure that both they and the pupil(s) running the social media account adhere to the acceptable use policies.

7. Personal use of social media (staff)

- Staff must only use school iPads or laptops for social media if used for work purposes (for example, department Instagram page).
- Staff must not use social media for personal use during timetabled lessons and tutor periods. While using social media, “liking” harmful content, or circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political views or promotion of outside organisations unrelated to School are also prohibited. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems.
- Staff should be aware that the DSL conducts network monitoring (in line with KCSIE) and any communication via school networks may be seen.
- Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.
- We prohibit staff from using their work email address for any personal use of social media.
- On leaving The Crypt School’s employment, staff members must not contact pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.
- Caution is advised when inviting or accepting work colleagues to be ‘friends’ or followers on personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships.
- Staff must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or The Crypt School.

8. Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Under no circumstances should staff share or upload pupil pictures online other than via School linked social media accounts.
- Any images shared featuring staff and pupils should be less vulnerable to exploitation by AI: for example, share lower quality images, pupils further away or sides and backs of heads rather than close up portraits.

- If anyone, for any reason, asks not to be filmed or photographed then their wishes must be respected.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately and ensure it is also deleted from deleted items.

9. The monitoring of social media

The contents of School IT resources and communications systems are our 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.

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by 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. We 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. GDPR regulations will be followed in this instance.

Do not use School IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

10. Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

11. Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.

- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school Protocols.

12. Social media and the end of employment

If a member of staff's employment with our School should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that you are no longer employed or associated with our School. If the departing member of staff had access to a school social media account, these passwords should be changed so they remain secure.

13. Recruitment

In line with Safer Recruitment, we will conduct internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

Links to other policies:

- Safeguarding
- Behaviour
- Anti-bullying and Hate
- Acceptable use agreements (Staff and Pupils)
- Staff code of conduct

Reviewed: June 2026

Approved by Headmaster: June 2026

Review cycle: Annual

Review Date: April 2027