



ROBERT CLACK SCHOOL

SOCIAL MEDIA AND SOCIAL NETWORKING POLICY

If printed, copied or otherwise transferred from this website this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time. Please consult the Policies page on the website for the latest update.

Controlled Document

Title	Social Media and Social Networking Policy
Author	Data Protection Enterprise Ltd
Owner	Headteacher
Version	Version 2
Updated	August 2026
Approved	Approved in accordance with the School's governance arrangements
Review date	August 2029 or earlier where there is a change in the applicable law affecting this Policy Guidance

Version Control

Version	Date	Author	Description of change
1	August 2024	Data Protection Enterprise Ltd	Original policy; reviewed August 2025.
2	August 2026	Data Protection Enterprise Ltd www.dpenterprise.co.uk	Policy review. Updated governance, safeguarding, data protection, official-account, personal-use, recruitment, AI/deepfake and smart-device provisions.

Contents

1. Purpose and principles
2. Scope and definitions
3. Roles and responsibilities
4. Access to social media
5. Official School accounts
6. Photographs, video, pupil work and personal data
7. Personal use by staff, governors and volunteers
8. Contact with pupils and former pupils
9. Pupils' use and online safety
10. Cyberbullying, harmful content and safeguarding concerns
11. Recruitment and social media checks
12. Monitoring, incidents and enforcement
13. Review and related policies

1. PURPOSE AND PRINCIPLES

Social media can support communication, learning, community engagement and the celebration of achievement. It can also create safeguarding, confidentiality, reputational, employment and data protection risks. This policy sets clear standards for safe, lawful and professional use.

The School will use social media in a way that:

- places the welfare and best interests of children first;
- protects privacy, confidentiality and the security of personal information;
- maintains professional boundaries and public confidence;
- supports freedom of expression only within the limits of lawful and professional conduct;
- meets safeguarding, political impartiality, equality and employment obligations; and
- reflects the School values.

2. SCOPE AND DEFINITIONS

This policy applies to employees, agency staff, governors, members, volunteers, contractors, pupils and any person communicating on behalf of the School. It applies to official and personal use where that use relates to the School, affects professional responsibilities, creates a safeguarding concern or may reasonably affect the School or.

‘Social media’ includes social networking, messaging, discussion and media-sharing services, including Facebook, Instagram, X, Threads, TikTok, Snapchat, YouTube, LinkedIn, WhatsApp, blogs, forums, livestreaming, gaming and community platforms, and future services with comparable functions.

The policy applies to posts, comments, reactions, direct messages, disappearing content, groups, livestreams, photographs, recordings, voice notes and content generated or altered using artificial intelligence. Private, restricted or temporary content may still be copied, shared, disclosed or become public.

3. ROLES AND RESPONSIBILITIES

3.1 Governing Board

- approves this policy and holds leaders to account for its implementation;
- ensures appropriate safeguarding, data protection and acceptable-use arrangements are in place.

3.2 Headteacher

- ensures staff understand this policy and receive appropriate training;
- authorises official accounts and assigns accountable owners;
- ensures concerns are investigated promptly under the appropriate safeguarding, disciplinary, complaints or behaviour procedure; and
- ensures proportionate monitoring, access controls and continuity arrangements are in place.

3.3 Designated Safeguarding Lead (DSL)

The DSL leads the safeguarding response to online concerns, including grooming, exploitation, sexual harassment, sharing of nudes or semi-nudes, sextortion, harmful or extremist content, impersonation and cyberbullying. Evidence must be preserved and managed in accordance with safeguarding procedures; staff must not investigate beyond their role.

3.4 Data Protection Officer (DPO)

The DPO advises on data protection compliance, privacy information, incidents, rights requests and whether a data protection impact assessment is required. Operational ownership and approval of communications remain with the School.

3.5 All users

All users must follow this policy, protect accounts and devices, report concerns promptly and cooperate with any lawful investigation.

4. ACCESS TO SOCIAL MEDIA

Personal use during working time must not interfere with duties, learning, safeguarding or the proper use of School resources. The School may restrict access on its network or devices. Limited personal use may be permitted during authorised breaks where local rules allow it.

Pupils may use only services, accounts and features authorised for an educational purpose, under appropriate supervision and in accordance with the Acceptable Use Policy. A blanket rule based solely on age is not appropriate: platforms set different minimum ages and services may change their terms. The School will consider the service's age requirements, educational purpose, privacy settings and safeguarding risks.

Access using School systems may be logged or monitored in accordance with the Acceptable Use Policy, privacy information and applicable law. Users should not expect personal use on School systems to be private.

5. OFFICIAL SCHOOL ACCOUNTS

An official account may be created only with written approval from the Headteacher or delegated communications lead. It must have a clear business purpose, named owner and deputy, and use an official email address. Personal accounts must not be used to conduct official School business.

Official accounts must:

- use strong unique passwords, multi-factor authentication where available and controlled recovery details;
- be recorded centrally, including platform, purpose, owner, administrators and recovery arrangements;
- have at least two authorised administrators wherever practicable, with access removed promptly when roles change;
- use approved branding and make clear which School, the account represents;
- use appropriate privacy, moderation, comment and direct-message settings;

- publish accurate, accessible and professional content and correct material errors promptly;
- not endorse personal commercial interests or promote partisan political views;
- avoid live location information or future details that could create a safeguarding or security risk;
- retain information that forms an official record in an approved School system rather than relying on the platform; and
- be reviewed periodically and closed securely when no longer required.

Direct messages must not be used for confidential casework, safeguarding reports, complaints, absence reporting or other matters requiring a secure formal record. The sender should be redirected to the appropriate approved channel and any necessary record transferred promptly. External organisations managing accounts on behalf of the School must be subject to appropriate written terms, due diligence, access controls, confidentiality, data protection and safeguarding requirements.

6. PHOTOGRAPHS, VIDEOS, PUPIL WORK AND PERSONAL DATA

The School must identify and document an appropriate lawful basis for material published through official accounts and explain the use clearly in its privacy information. Where the School relies on public task for routine celebration and promotion of educational provision, it will provide a clear and effective opportunity to object or opt out and will respect recorded choices. Consent must be used where the particular processing genuinely requires it and must be capable of being withdrawn.

Before publication, authorised staff must check:

- the pupil's and, where appropriate, parent/carer's recorded preference;
- whether publication could identify a looked-after child, child subject to safeguarding measures, or any person whose location or identity requires protection;
- that names, uniforms, location data, timetables, badges, documents and background information do not create unnecessary risk;
- that the content is respectful, proportionate and suitable for a potentially permanent and global audience; and
- that copyright, ownership and accessibility requirements have been considered.

Images or recordings for official publication should be captured and stored using School-approved devices and systems. Personal devices must not be used unless expressly authorised for a defined exceptional purpose, with appropriate security controls and prompt transfer to an approved system followed by verified deletion from the device and any cloud backup.

Smart glasses, body-worn cameras, covert recording devices and other wearable recording technology must not be used to capture School activity unless specifically authorised under a separate documented process. AI tools must not be used to create, alter or publish realistic images, voices or videos of identifiable pupils or staff unless the use has been approved and assessed as lawful, fair, transparent and safe. Misleading synthetic or 'deepfake' content is prohibited.

Parents, carers and visitors may be asked not to publish images or recordings containing other people's children. Any restriction imposed at an event will be explained and enforced as an event, safeguarding or behaviour rule, rather than represented as a general data protection prohibition on personal photography.

7. PERSONAL USE BY STAFF, GOVERNORS AND VOLUNTEERS

People connected with the School have private lives and rights to expression. Those rights carry responsibilities where conduct is connected to their role, affects safeguarding or working relationships, discloses confidential information, breaches the law or may seriously damage confidence in the School.

Users must not, through personal accounts:

- disclose or discuss confidential information about pupils, families, colleagues, governors or School business;
- post photographs, recordings or pupil work obtained through their role;
- present personal views as those of the School, or use official logos without authority;
- engage in harassment, discrimination, bullying, hate speech, threats, defamation or unlawful conduct;
- post content that compromises safeguarding, professional boundaries, political impartiality or their ability to carry out their role;
- use personal messaging or social-media accounts for routine communication with pupils or parents in their professional capacity; or
- use confidential School information in prompts to generative AI services or upload it to unapproved platforms.

Privacy settings are recommended but do not remove professional obligations. Users should assume that content may be copied or shared. Staff are not required to monitor pupils, parents or colleagues through personal accounts and should not conduct their own online investigation into a concern. A personal disclaimer may help distinguish private views, but it does not excuse a breach of confidentiality, safeguarding duties, professional standards or this policy.

8. CONTACT WITH PUPILS AND FORMER PUPILS

Staff, volunteers and governors must not add, follow, message or communicate with current pupils through personal accounts, except where a pre-existing family relationship makes contact unavoidable and the circumstances have been declared and managed appropriately. Contact for School purposes must use approved platforms and accounts and remain transparent, necessary and capable of oversight.

The same caution applies to former pupils, particularly while they remain under 18 or where a power imbalance, safeguarding concern or professional boundary continues. Staff should not assume that a pupil leaving the School immediately makes personal contact appropriate.

Any attempted inappropriate contact, sexualised communication, grooming concern or boundary breach must be reported immediately under safeguarding and low-level concerns/allegations procedures. Staff must not delete relevant messages unless instructed after evidence has been secured.

9. PUPILS USE AND ONLINE SAFETY

Online safety education will be age appropriate and embedded through the curriculum, assemblies and wider safeguarding work. Pupils will be taught about privacy, respectful communication, misinformation, algorithms, scams, grooming, exploitation, extremist content, sharing images,

livestreaming, gaming and messaging risks, sexual harassment, sextortion, impersonation, AI-generated content and how to report concerns.

Pupils must not use social media to bully, threaten, impersonate, discriminate against or humiliate others; share private or sexual content; publish recordings made without authority; access or distribute illegal or harmful material; or interfere with School accounts or systems.

The School will work with parents and carers to promote safe use. Platform age limits will be explained accurately; the age of 13 in UK data protection law relates specifically to a child's ability to consent to an online service's processing where that service relies on consent and is not a universal minimum age for every platform or use.

10. CYBERBULLYING HARMFUL CONTENT AND SAFEGUARDING CONCERNS

The School will respond to online behaviour where it affects a pupil's welfare, the orderly running of the School, the safety of the School community or the reputation and working relationships necessary to provide education. This may include conduct originating away from the premises and outside School hours.

Concerns must be reported promptly to the DSL, Headteacher or line manager as appropriate. Where there is immediate danger, contact emergency services. The School may also report content to a platform, police, local authority or other relevant body and will support affected individuals. Evidence should be preserved carefully, for example by recording URLs, usernames, dates and screenshots where safe and lawful. Staff must not forward sexual images of children, create additional copies unnecessarily or ask a child to resend content. The safeguarding procedure for sharing nudes and semi-nudes must be followed.

11. RECRUITMENT AND SOCIAL MEDIA CHECKS

The School will not carry out informal or speculative searches of applicants' personal social media. If public online or social-media checks are considered necessary for a particular role or identified risk, they must form part of an approved, documented and transparent recruitment process.

Candidates must be told in advance. The scope must be necessary and proportionate, only relevant information may be considered, and checks should be undertaken by a person who is not the final decision-maker wherever practicable. Information revealing protected characteristics or irrelevant private matters must not influence selection. Any concern relied upon should be verified and the candidate given an appropriate opportunity to respond.

12. MONITORING, INCIDENTS AND ENFORCEMENT

The School may monitor official accounts, public references to the School and use of its systems for legitimate safeguarding, security, reputation and operational purposes. Monitoring will be necessary, proportionate, transparent and not used as unjustified surveillance of private life.

Suspected compromise, impersonation, accidental disclosure, unauthorised posting or loss of control of an account must be reported immediately under the Security Incident and Data Breach Policy. Passwords or access tokens should be changed promptly, evidence preserved, and the DPO consulted where personal information may be affected.

Breaches may be addressed under safeguarding, disciplinary, capability, behaviour, complaints, governance or contractual procedures. Action will be fair and proportionate and will consider context, actual or potential harm, role, intent, previous advice and professional obligations. Nothing in this policy prevents lawful whistleblowing, protected disclosures, trade union activity or reporting concerns to an appropriate authority.

13. REVIEW AND RELATED POLICIES

The DPO will advise on data protection aspects of this policy. The policy owner is responsible for implementation and review. An interim review may be triggered by a significant incident or a change in legislation, statutory guidance, platform functionality, technology or identified risk.

This policy should be read with the School's:

- Safeguarding and Child Protection Policy;
- Online Safety and Acceptable Use Policies;
- Staff Code of Conduct and low-level concerns/allegations procedures;
- Data Protection and Privacy Notices;
- Photography and Images Policy;
- Recording Meetings/Calls Policy;
- Security Incident and Data Breach Policy;
- Information Security Policy;
- Behaviour and Anti-Bullying Policies;
- Complaints, Whistleblowing, Disciplinary and Recruitment Policies; and
- Artificial Intelligence Policy, where adopted.

Key external guidance:

[Keeping children safe in education 2026 \(effective 1 September 2026\)](#)

[ICO – Children and the UK GDPR](#)

[ICO – Taking photographs: advice for schools](#)