Wolsey House Primary School

Social Media and Electronic Communications Policy

Policy date: October 2026

Policy review date: October 2027

Together we grow, achieve and thrive.

1. Introduction and scope

1.1 This policy forms part of the school's commitment to safeguarding, staff wellbeing, professional conduct, information security and its duty of care.

It applies to all school employees and to their use of social media and electronic communications:

- during working time;
- using school-owned equipment, systems, accounts or networks;
- when communicating in connection with school business; and
- outside work where there is a genuine and proportionate connection with their employment.

Conduct outside work may be considered under this policy where it:

- raises a safeguarding concern;
- calls into question the employee's suitability to work with children;
- breaches confidentiality, data-protection requirements or professional boundaries;
- involves unlawful, discriminatory, harassing or otherwise seriously inappropriate conduct;
- materially affects the employee's ability to perform their role; or
- causes, or is reasonably likely to cause, material harm to the school, its pupils, staff or reputation.

Any concerns about conduct outside work will be considered fairly and proportionately, taking account of the circumstances, the employee's role, their right to a private life and freedom of expression, and the effect or potential effect of the conduct on their employment or the school.

The relevant principles of this policy will also apply, where appropriate, to agency workers, contractors, volunteers, governors and others undertaking work or duties on behalf of the school.

1.2 This policy forms part of the school's online-safety and safeguarding framework. It should be read alongside the Online Safety Policy, Staff Code of Conduct and the relevant Acceptable Use Agreement.

1.3 For the purposes of this policy, "social media" means any website, application, platform or online service that enables users to create, publish, communicate, comment on or share information, opinions, images, audio, video or other content.

This includes, but is not limited to:

- social-networking and professional-networking platforms;
- video- and image-sharing services;
- blogs, forums and online communities;
- messaging applications and group chats;
- livestreaming and gaming platforms; and
- collaborative or content-sharing services.

"Electronic communications" includes email, text messages, instant messaging, group messaging, video conferencing, online meetings and other communication sent or received through an electronic device, account, platform or system.

1.4 Technology and social-media platforms change frequently. This policy therefore applies to all current and future forms of social media and electronic communication, whether accessed through a

school or personal device, account or network, where the use has a connection with the employee's work or the school.

1.5 Social media and electronic communications provide valuable opportunities for professional communication, collaboration, teaching and learning. Their inappropriate or insecure use may, however, create safeguarding, professional, legal, employment, data-protection and reputational risks.

The purposes of this policy are to:

- safeguard pupils, staff and members of the school community;
- maintain appropriate professional boundaries;
- protect confidential and personal information;
- promote secure, lawful and responsible use of technology;
- protect staff from avoidable risks, including allegations, harassment, impersonation, phishing and compromised accounts;
- provide clear expectations about professional and personal use;
- ensure that teachers' use of social media and electronic communications is consistent with Part Two of the Teachers' Standards;
- protect the legitimate interests and reputation of the school; and
- enable concerns about conduct to be considered fairly, consistently and proportionately.

1.6 This policy should be read alongside the following school policies and procedures, where relevant:

- Staff Code of Conduct;
- Safeguarding and Child Protection Policy;
- Online Safety Policy;
- Acceptable Use Agreements;
- Use of Artificial Intelligence Policy;
- Data Protection Policy and Privacy Notices;
- Records Management and Retention Policy;
- Behaviour Policy;
- Anti-Bullying Policy;
- Allegations Against Staff and Low-Level Concerns Procedures;
- Whistleblowing Policy;
- Disciplinary Procedure;
- Grievance Procedure; and
- Complaints Policy.

1.7 This policy will be applied in accordance with relevant employment, safeguarding, equality, human-rights and data-protection legislation; statutory safeguarding guidance; the Teachers' Standards; ACAS guidance; and applicable national and local terms and conditions of employment.

All staff must follow the school's safeguarding arrangements and report any safeguarding concern arising through social media or electronic communication without delay, in accordance with the Safeguarding and Child Protection Policy and the school's allegations and low-level concerns procedures.

2. Equality, wellbeing and support

2.1 The school will apply this policy fairly, consistently and without unlawful discrimination, harassment or victimisation because of age, disability, gender reassignment, marriage or civil partnership, pregnancy or maternity, race, religion or belief, sex or sexual orientation.

The Headteacher will ensure that employees are given an appropriate opportunity to understand and participate in any process conducted under this policy. Supportive measures will be considered where appropriate, taking account of the employee's individual circumstances.

2.2 The school will take proactive steps to prevent discrimination, harassment, sexual harassment and victimisation through electronic communications and online activity.

From 30 October 2026, the school will take all reasonable steps to prevent sexual harassment of its employees and will comply with its duties concerning harassment of employees by third parties. This includes considering risks arising through email, messaging applications, social media, online meetings and other digital communication.

Employees must report discriminatory, harassing or sexually harassing online conduct promptly through the appropriate management, grievance, safeguarding or whistleblowing procedure. The school will take concerns seriously and will consider appropriate support, protective measures and further action.

2.3 The school will make reasonable adjustments for disabled employees where required by the Equality Act 2010. This includes considering adjustments to meetings, communications, timescales and other procedures under this policy where an employee would otherwise experience a substantial disadvantage.

The duty may arise where the school knows, or could reasonably be expected to know, that an employee is disabled. Employees are encouraged to tell the Headteacher or another appropriate manager about any support or adjustment they may need. Requests will be considered sensitively, individually and, where appropriate, with advice from human resources or occupational health.

2.4 The school recognises its responsibility to assess and manage risks to employees' health and safety, including risks arising from work-related stress, and to take reasonably practicable steps to address identified risks.

When applying this policy, the school will have regard to the employee's health and wellbeing and will consider appropriate support. This does not prevent the school from addressing legitimate safeguarding, conduct, capability or employment concerns.

2.5 The school recognises that neurodivergent employees may experience workplace practices, communication or formal procedures differently. Neurodivergence may amount to a disability under the Equality Act 2010, depending on its effect on the individual, but a formal diagnosis is not required before support can be discussed or provided.

Where the school is aware that an employee is neurodivergent or may require support, the Headteacher or appropriate manager will discuss their individual needs with them and consider appropriate support and any reasonable adjustments. Depending on the circumstances, these might include:

- providing information or questions in advance;
- using clear and unambiguous written communication;
- allowing additional time to read, process or respond to information;
- permitting a companion or other agreed support where appropriate;

- holding meetings in a suitable environment;
- providing breaks during longer meetings; or
- agreeing an alternative method of communication.

Any adjustments will be tailored to the employee and kept under appropriate review.

3. Internet and network use

3.1 The internet is a valuable resource for teaching, learning, communication and professional development. Its use may also create safeguarding, cyber-security, data-protection and professional risks. Employees must therefore use the internet, school systems and school equipment safely, responsibly and in accordance with this policy, the Online Safety Policy and the relevant Acceptable Use Agreement.

3.2 School equipment, accounts, systems and networks are provided primarily for work-related purposes. Any personal use must be limited, reasonable and permitted under the school's Acceptable Use Agreement or specifically authorised by the Headteacher. Personal use must not:

- interfere with the employee's work or the work of others;
- incur an unreasonable cost to the school;
- compromise the security or operation of school systems;
- involve access to unlawful, offensive or otherwise inappropriate material;
- breach confidentiality, safeguarding or data-protection requirements; or
- bring the school into disrepute.

Where the school does not permit personal use, this will be made clear within the Acceptable Use Agreement.

3.3 The school may monitor the use of its equipment, systems, accounts and networks for legitimate purposes, including safeguarding, cyber security, system management, regulatory compliance and investigating suspected misuse.

Any monitoring will be undertaken in accordance with section 9 of this policy, the school's privacy information and applicable data-protection requirements. Monitoring will be transparent, necessary and proportionate, and employees will be informed about its nature, purpose and extent.

Employees should not assume that activity carried out using school equipment, systems, accounts or networks is private. However, this does not permit indiscriminate or excessive monitoring.

3.4 Employees must not attempt to disable, bypass or interfere with the school's filtering, monitoring, security or access-control systems. If an employee believes that access to a blocked website or service is required for a legitimate educational or professional purpose, they must follow the school's approved process for requesting access.

3.5 Employees must exercise caution when opening links, attachments, downloads or messages, particularly where the source is unknown or unexpected. Suspected phishing, malware, fraudulent messages, compromised accounts or other cyber-security incidents must be reported immediately to the school's designated IT contact and, where relevant, the Designated Safeguarding Lead or Data Protection Officer.

If inappropriate or potentially unlawful material is accessed accidentally, the employee must stop viewing it and report it immediately in accordance with the Online Safety Policy. They must not copy, forward, save or share the material unless specifically instructed to preserve evidence by an

appropriate senior leader, the DSL, police or another authorised agency. Nothing in this paragraph permits an employee to make, copy, download or store suspected child sexual abuse material. The requirements in section 7.9 must always be followed.

3.6 Employees who are unsure about the appropriate use of the internet or school technology should seek advice from the Headteacher, Online Safety Lead, Designated Safeguarding Lead or designated IT support.

The UK Safer Internet Centre's Professionals Online Safety Helpline may also provide advice to professionals working with children and young people:

- Telephone: 0344 381 4772
- Email: helpline@saferinternet.org.uk

The helpline does not replace the school's safeguarding procedures. Any concern about a child's safety or welfare must be reported immediately in accordance with the Safeguarding and Child Protection Policy.

4. Email use

4.1 Approved accounts

Employees must use their school email account or another school-approved communication system for school business. Personal email accounts must not be used to communicate with pupils or parents and carers, or to send, receive or store confidential school information.

School emails must not be automatically forwarded to a personal email account. Employees must protect their account credentials, use multi-factor authentication where provided and report any suspected unauthorised access or compromised account immediately.

4.2 Professional and responsible communication

Emails sent or received in connection with school business form part of the school's records. They may be disclosable under data-protection legislation, freedom of information requirements, legal proceedings, safeguarding enquiries or employment procedures.

Employees must ensure that emails are:

- professional, respectful, factual and capable of being justified;
- limited to information that is necessary for the intended purpose;
- addressed only to the appropriate recipients;
- consistent with confidentiality, safeguarding and data-protection requirements; and
- retained or deleted in accordance with the school's records-retention arrangements.

Employees should write emails on the basis that they may subsequently be read by the person concerned or disclosed to an authorised third party.

4.3 Communication with pupils

Electronic communication with pupils must only take place through an approved school email account, learning platform or other school-authorised system. Employees must not use personal email accounts, personal telephone numbers, personal social-media accounts or personal messaging applications to communicate with pupils.

Communication must have a clear educational or pastoral purpose, maintain appropriate professional boundaries and comply with the Staff Code of Conduct, Online Safety Policy and Safeguarding and Child Protection Policy.

4.4 Managing email workload

Email is a valuable form of communication, but unnecessary or poorly targeted emails can increase workload. Before sending an email, employees should consider:

- whether the email is necessary;
- whether email is the most appropriate method of communication;
- whether a meeting, telephone call or conversation would be more effective;
- whether a response is required and, if so, make this clear;
- whether every intended recipient needs to receive the message; and
- whether the matter could be included in an established briefing, bulletin or team communication.

4.5 Preparing and sending emails

Before sending an email, employees must:

- check that all recipients are correct;
- use the "reply all" function only where every recipient needs the response;
- use the blind carbon copy—or BCC—field where appropriate to protect recipients' email addresses;
- use a clear and concise subject line;
- avoid placing confidential or sensitive personal information in the subject line;
- keep the message clear, concise and professional;
- check attachments and sharing permissions;
- share large internal files through an approved system such as Microsoft Teams or OneDrive rather than attaching them to an email; and
- take additional care before sending confidential or special-category personal information.

Where a message or attachment contains confidential information, employees must use the secure method approved by the school and check the recipient's address carefully before sending it.

4.6 Email times and availability

In accordance with the Staff Handbook:

- staff should check their school email account on each of their working days;
- staff must not routinely check or respond to emails during lesson time;
- emails should be sent between 07:00 and 18:00 Monday to Thursday and between 07:00 and 16:00 on Friday; and
- emails should not ordinarily be sent during weekends or bank holidays.

Where an employee prepares an email outside these times, they should use the scheduled-send function so that it is delivered during the permitted hours.

There is no expectation that employees will read or respond to routine emails outside their normal working hours, during weekends, bank holidays, periods of authorised absence or on days when a part-time employee does not work.

Part-time employees should use an appropriate automatic reply stating their usual working days and when the message is likely to be considered. Automatic replies must not disclose unnecessary personal information or information that could create a security risk.

The above restrictions do not prevent authorised emergency, safeguarding, business-continuity or other genuinely urgent communications.

4.7 Responding to parents and carers

Emails from parents and carers should normally be acknowledged within one working day. Where a full response requires investigation, consultation or consideration, the acknowledgement should explain that the matter is being considered and, where possible, indicate when a fuller response can be expected.

Employees are not expected to respond outside their normal working hours or on non-working days. Urgent safeguarding concerns must be dealt with immediately through the school's safeguarding procedures rather than left to await a routine email response.

Repeated, excessive, abusive or otherwise unreasonable email contact must be referred to the employee's line manager or the Headteacher and managed in accordance with the school's relevant communication, complaints or persistent and vexatious complaints procedures.

4.8 Safeguarding and security

Employees must exercise caution when opening links, attachments or messages, particularly where the sender or content is unexpected. Suspected phishing, malware, fraudulent messages, data breaches or compromised accounts must be reported immediately through the school's designated reporting procedure.

Email must not be relied upon as the sole method of reporting an urgent safeguarding concern. Employees must follow the school's Safeguarding and Child Protection Policy and ensure that the concern is brought promptly to the attention of the DSL or a deputy.

5. Messaging and other internet-based communications

5.1 Approved communication systems

School business must normally be conducted through school-approved systems, such as school email, Microsoft Teams, CPOMS or another platform specifically authorised for the relevant purpose.

Personal messaging accounts and applications, including WhatsApp, must not be used to:

- communicate with pupils;
- store or share confidential information about pupils, parents, carers or employees;
- discuss safeguarding concerns or individual pupil cases;
- share photographs, videos, voice recordings or personal information relating to pupils;
- communicate formal decisions or instructions that need to form part of the school's records; or
- transfer school documents or information to personal devices or accounts.

5.2 Informal staff messaging groups

Employees may choose to participate in informal staff messaging groups, including WhatsApp groups, for limited and non-confidential purposes, such as voluntary social arrangements or brief practical updates.

Participation must be voluntary. Employees who do not wish to join or who leave an informal group must not be disadvantaged and must continue to receive all information needed to carry out their role through an approved school communication system.

Informal messaging groups must not become the only means through which rotas, changes to working arrangements, safeguarding information, management instructions or other essential school information are communicated.

Unless specifically authorised by the school for an emergency or business-continuity purpose, employees should not be expected to read or respond to messages outside their normal working hours.

5.3 Standards of conduct

When communicating with colleagues through any electronic platform, employees must:

- maintain a professional and respectful tone when discussing work-related matters;
- avoid comments that are discriminatory, harassing, sexually harassing, bullying, abusive, defamatory or otherwise inappropriate;
- avoid personal criticism, gossip or speculation about colleagues, pupils or families;
- consider carefully whether an image, recording, link, joke, emoji or other content is appropriate before sending it;
- respect the privacy and personal information of group members;
- obtain permission before adding an employee to a group or sharing their personal telephone number;
- avoid sharing messages, images or screenshots outside the group without a legitimate reason and appropriate authority; and
- remember that messages may be copied, forwarded, disclosed or retained as evidence.

The same standards of professional conduct apply to messages, images, audio, video, GIFs, emojis, reactions and AI-generated or digitally altered content.

5.4 Microsoft Teams and other approved platforms

School-approved platforms such as Microsoft Teams must be used only in accordance with their authorised purpose and the school's Acceptable Use Agreement.

Employees must:

- use their school account;
- ensure that messages are sent to the correct person, group or channel;
- maintain appropriate professional boundaries and language;
- check access permissions before sharing documents;
- share personal or confidential information only where necessary, proportionate and permitted for that platform;
- use CPOMS for safeguarding records;
- retain formal decisions and records in the appropriate school system; and
- comply with the school's records-retention and deletion arrangements.

The availability of a private chat function does not make it appropriate for confidential casework, safeguarding discussions or informal commentary about individuals.

5.5 Accidental disclosure and security incidents

If information is sent to the wrong person or group, confidential information is shared inappropriately, or an account or device may have been compromised, the employee must report this immediately to the Headteacher or designated senior leader and the school's Data Protection Officer or IT support, as appropriate.

Employees should preserve relevant evidence, such as the message, date, time and screenshots, unless doing so would involve unnecessarily copying illegal or harmful content. They must not attempt to conceal the incident or rely solely on deleting the message.

6. Data protection, freedom of information and copyright

6.1 Data protection

Employees must handle personal information in accordance with the UK GDPR, the Data Protection Act 2018, the school's Data Protection Policy, privacy notices, records-retention arrangements and any relevant school procedures.

Employees must:

- access, use and share personal information only where necessary for an authorised school purpose;
- use school-approved systems and accounts;
- keep information accurate, relevant and limited to what is needed;
- protect confidential and special-category personal data;
- check recipients, attachments and access permissions before sharing information;
- retain and securely delete information in accordance with the school's retention schedule; and
- follow the school's procedures when taking, storing, using or publishing photographs and recordings.

Personal information must not be stored or transferred through personal email accounts, personal cloud storage, personal messaging applications or unauthorised devices or platforms.

6.2 Information requests

Employees should be aware that emails, messages, documents and other records created in connection with school business may be relevant to:

- a subject access request;
- a freedom of information request;
- a request for a pupil's educational record;
- a complaint, safeguarding enquiry or employment procedure;
- legal proceedings; or
- another lawful disclosure requirement.

Any request for information must be forwarded promptly to the Headteacher, Data Protection Officer or other designated person in accordance with the school's procedures. Employees must not respond independently unless authorised to do so.

Once an employee becomes aware of an information request, complaint, investigation or legal hold, they must not delete, alter, conceal or destroy potentially relevant records.

6.3 Monitoring information

Personal data obtained through the monitoring of school equipment, systems, accounts or networks will be processed in accordance with data-protection legislation, the school's Data Protection Policy, applicable privacy information and section 9 of this policy.

Monitoring information will:

- be collected for a defined and legitimate purpose;
- be limited to what is necessary and proportionate;
- be held securely;
- be accessed only by authorised individuals;
- not be retained for longer than necessary; and
- be disclosed only where there is a lawful and legitimate reason.

6.4 Personal data breaches

A personal data breach may include the loss, unauthorised disclosure, alteration or destruction of personal information, or unauthorised access to it. Examples include:

- sending an email or attachment to the wrong recipient;
- losing a device or document;
- sharing information through an unauthorised platform;
- disclosing recipients' email addresses inappropriately;
- unauthorised access to an account; or
- publishing a photograph or personal information incorrectly.

An actual or suspected breach must be reported immediately in accordance with the Data Protection Policy. Employees must preserve relevant information, follow any instructions given and must not attempt to conceal or investigate the matter themselves beyond taking immediate steps to limit further disclosure.

The Data Protection Officer or other authorised person will determine whether the breach must be reported to the Information Commissioner's Office or affected individuals. Inappropriate access, use or disclosure may also be addressed under the school's Disciplinary Procedure.

6.5 Copyright and intellectual property

Material available on the internet is not automatically free to copy, adapt, publish or share. Employees must respect copyright, licensing conditions and other intellectual-property rights when using text, images, photographs, music, video, software or other content.

Material may only be copied, adapted, uploaded, published or shared where at least one of the following applies:

- the school or employee owns the relevant rights;
- permission has been obtained from the rights holder;
- the use is covered by a licence held by the school;
- the material is subject to an appropriate open licence, such as a relevant Creative Commons licence, and its conditions are followed; or
- the use falls within an applicable statutory copyright exception.

Where required, the creator and source must be acknowledged. Employees must not remove copyright notices, watermarks or attribution information.

The school's educational purpose does not automatically permit unrestricted copying or online publication. School licences and educational exceptions have specific limits and conditions.

6.6 Links to online material

Employees may link to material that has been lawfully published online where doing so is appropriate and does not breach safeguarding, confidentiality or security requirements.

Employees must not link to material where they know, or reasonably suspect, that it has been published unlawfully, or where the link is intended to bypass a paywall, login requirement or other access restriction.

6.7 Checks before publishing or sharing

Before publishing, uploading or sharing material electronically, employees must consider:

- whether there is a legitimate school purpose;
- whether the intended audience and access settings are appropriate;
- whether the platform is approved and sufficiently secure;
- whether the material contains personal, confidential or safeguarding information;
- whether the school has an appropriate lawful basis for processing any personal data;
- whether any required parental or pupil information, agreement or consent arrangements have been followed;
- whether the school owns the material or has permission, a licence or another lawful basis to use it;
- whether any attribution or copyright notice is required; and
- whether publication could compromise the safety, dignity or privacy of a pupil, employee or other person.

The use of artificial intelligence to create, adapt or reproduce content must comply with the school's Use of Artificial Intelligence Policy. Employees remain responsible for checking that AI-generated content does not breach copyright, confidentiality, data-protection or safeguarding requirements.

7. Social media

7.1 General principles

Social media forms part of many people's personal and professional lives. The school respects employees' rights to a private life and freedom of expression. However, social-media activity may have safeguarding, professional, employment, data-protection and reputational consequences.

This section applies to personal and school-managed accounts, public and private groups, comments, posts, messages, images, recordings, livestreams, reactions and content that an employee creates, shares, forwards or endorses.

7.2 Privacy and permanence

Employees should not assume that social-media communication is private, temporary or restricted to its intended audience. Content may be copied, altered, searched, forwarded, downloaded or shared without the author's knowledge.

Privacy settings reduce risk but do not guarantee confidentiality. Employees should review their privacy, location, tagging and security settings regularly and consider carefully before publishing or sharing content.

7.3 Personal social-media accounts

Employees may identify their occupation or employer on a personal or professional profile where they choose to do so. However, they must not:

- present personal views as those of the school;
- use the school's name, logo, branding or images in a way that suggests official authorisation;
- disclose confidential, personal or safeguarding information;
- publish content about individual pupils, parents, carers, colleagues or school matters without authority;
- post from school premises in a way that reveals confidential information, pupil identities or security arrangements;
- make discriminatory, harassing, sexually harassing, bullying, threatening, defamatory or otherwise unlawful comments; or
- engage in conduct that has a genuine and proportionate connection with their employment and raises safeguarding or professional-suitability concerns or creates a material risk of harm to the school, its pupils, staff or reputation.

Employees should make clear, where appropriate, that views expressed through a personal account are their own. A disclaimer does not, however, remove responsibility for inappropriate conduct.

7.4 Contact with pupils

Employees must not use personal social-media accounts to:

- send or accept friend, follow or connection requests from current pupils;
- exchange private or direct messages with pupils;
- join pupil-managed groups or chats;
- monitor pupils' accounts without an authorised safeguarding reason; or
- establish or maintain personal online relationships with pupils.

If a pupil attempts to contact an employee through a personal account, the employee must not engage in conversation. They should preserve appropriate evidence and report the contact to the Designated Safeguarding Lead where it raises a safeguarding, boundary or welfare concern.

Any necessary electronic communication with pupils must take place through a school-approved account or platform and for an authorised educational or pastoral purpose.

7.5 Parents, carers, relatives and existing relationships

Employees should not ordinarily use personal social-media accounts to establish new relationships with parents or carers whom they know solely through their professional role.

The school recognises that employees may have legitimate pre-existing relationships with parents or carers through family, friendship or the local community. Employees should maintain appropriate professional boundaries and must not discuss pupils, colleagues, complaints, safeguarding matters or other confidential school business through personal accounts.

Where an employee is related to a pupil, parent or carer, or where an existing relationship could create an actual or perceived conflict of interest, the employee should inform the Headteacher so that any necessary safeguards can be considered.

Particular caution must be exercised in relation to former pupils, especially where they are under 18, remain connected with current pupils or where the previous position of trust remains relevant.

7.6 School-related groups and pages

Where employees participate in a social-media group or page referring to the school, their conduct must remain consistent with this policy and the Staff Code of Conduct.

Employees must not assume that a closed or private group is confidential. They must not use such groups to:

- disclose confidential or personal information;
- criticise or discuss identifiable pupils, families or colleagues;
- conduct safeguarding case discussions;
- circulate rumours, complaints or employment matters; or
- communicate formal school decisions or instructions.

Unauthorised accounts, groups or pages must not be created in the school's name or using its branding.

7.7 Official school social-media accounts

An official school social-media account may only be created with the Headteacher's approval. The school will retain ownership and control of all official accounts, content, contact details and access credentials.

Official accounts must:

- have a clearly defined educational or communication purpose;
- use a school-controlled email address;
- have at least two authorised administrators where practicable;
- use strong, unique passwords and multi-factor authentication where available;
- have documented arrangements for password recovery and changes in staffing;
- be operated only by authorised employees;
- comply with the school's publication, safeguarding and data-protection arrangements; and
- be monitored and reviewed appropriately.

Employees must not use their personal account to administer an official school account where this would expose personal information or undermine school ownership and control.

7.8 Photographs, recordings and digital content

Photographs, videos or audio recordings of pupils must only be taken, stored and published through school-approved devices, accounts and systems and in accordance with the school's data-protection, safeguarding and photographic-image arrangements.

Employees must not publish images or recordings that:

- identify a pupil contrary to the school's arrangements;
- reveal confidential, medical, safeguarding or location information;

- compromise a pupil's dignity or safety;
- expose security arrangements or confidential material visible in the background; or
- have been digitally altered or presented in a misleading or harmful way.

Employees must not create, request, share or endorse AI-generated or manipulated images, audio, video or "deepfake" content involving pupils, colleagues or members of the school community unless this has been expressly authorised for a legitimate educational purpose and complies with the Use of Artificial Intelligence Policy.

7.9 Safeguarding concerns identified online

Employees must not conduct their own investigation by attempting to access a pupil's private account, using another person's account, creating a false identity or making unauthorised contact.

Where an employee becomes aware of online material that may indicate a safeguarding concern, they must:

- report it immediately to the DSL or a deputy;
- record how and when the information came to their attention;
- preserve proportionate evidence, such as the web address, username, date, time or screenshot, where it is safe and lawful to do so;
- avoid commenting on, sharing, forwarding or otherwise increasing circulation of the material; and
- follow any instructions from the DSL, police or children's social care.

Employees must not make, copy or store an image of suspected child sexual abuse material. They should secure the device or page without further viewing and seek immediate advice from the DSL.

7.10 Security incidents, impersonation and online abuse

Employees must report immediately any:

- suspected compromise of a personal account used in connection with the school;
- compromise of an official school account;
- false or impersonation account involving the school, an employee or a pupil;
- threatening, abusive or harassing online communication;
- unauthorised publication of school information; or
- harmful AI-generated or manipulated content.

Relevant evidence should be preserved, but employees should not respond, retaliate or attempt to investigate the matter themselves. The school will consider appropriate safeguarding, employment, platform-reporting, data-protection and police action.

8. Artificial intelligence

8.1 Artificial intelligence—or AI—refers to computer systems designed to perform tasks that would ordinarily require aspects of human intelligence, such as recognising patterns, analysing information, making predictions or generating content.

Generative AI refers to tools that can create new text, images, audio, video, computer code or other content in response to instructions or prompts.

8.2 The school recognises that AI may support teaching, learning, accessibility, administration and staff workload when it is used safely and appropriately. Its use also creates potential risks relating to:

- inaccurate, fabricated or outdated information;
- bias and discrimination;
- safeguarding and harmful content;
- confidentiality and data protection;
- copyright and intellectual property;
- cyber security;
- over-reliance and loss of professional judgement;
- academic integrity;
- impersonation, manipulated media and deepfakes; and
- misleading representations of an individual's work or capabilities.

Detailed expectations for the selection, approval and use of AI are set out in the school's Use of Artificial Intelligence Policy.

8.3 Approved use

Employees must only use AI tools for school-related purposes where:

- the tool and proposed use have been approved by the school;
- the use is consistent with the Use of Artificial Intelligence Policy and other relevant school policies;
- appropriate safeguarding, data-protection and cyber-security considerations have been addressed;
- any relevant age restrictions and terms of use are followed; and
- the employee has sufficient knowledge and understanding to use the tool safely.

The introduction of a new AI tool or a materially different use of an existing tool must be referred to the Headteacher or designated AI lead. Advice from the Data Protection Officer or IT lead, and a data-protection impact assessment or other risk assessment, will be obtained where appropriate.

8.4 Personal and confidential information

Employees must not enter, upload or disclose personal, special-category, confidential, commercially sensitive or safeguarding information through an AI tool unless the specific tool and use have been expressly authorised by the school and all necessary data-protection safeguards are in place.

This includes information that directly or indirectly identifies:

- a pupil;
- a parent or carer;
- an employee;
- a governor or volunteer; or
- another member of the school community.

Removing a name may not be sufficient to anonymise information if the person could still be identified from the remaining details.

Employees must not upload pupil records, safeguarding records, medical information, staff records, assessment information, photographs, recordings, complaints or confidential school documents to an unauthorised AI tool.

These requirements apply during and outside working hours and regardless of whether the employee uses a school or personal account, device or internet connection.

8.5 Professional responsibility and human oversight

Employees remain professionally responsible for any content they create, adapt, use or share with the assistance of AI.

Before using AI-generated content, employees must check its:

- accuracy and reliability;
- curriculum relevance and age appropriateness;
- language, tone and accessibility;
- potential bias or discrimination;
- safeguarding implications;
- copyright and licensing position; and
- compliance with school policy.

AI output must not be treated as an authoritative source merely because it appears confident or convincing.

AI must not make, or be relied upon as the sole basis for, decisions about safeguarding, behaviour, assessment, SEND provision, employment or any other matter that could significantly affect an individual. Appropriate professional judgement and meaningful human oversight must always be maintained.

Where required by the school, employees must be transparent about their use of AI and appropriately acknowledge or record its use.

8.6 Safeguarding and inappropriate use

Employees must not use AI to create, alter or share content that:

- bullies, humiliates, harasses or discriminates against another person;
- sexualises a child or adult;
- falsely represents a real person;
- creates an unauthorised deepfake or impersonation;
- facilitates grooming, exploitation, coercion or criminal activity;
- breaches professional boundaries; or
- compromises the dignity, privacy or safety of a pupil, colleague or other person.

Any AI-related safeguarding concern must be reported immediately to the DSL or a deputy in accordance with the Safeguarding and Child Protection Policy.

8.7 Reporting concerns

Employees must report immediately any suspected:

- disclosure of personal or confidential information to an AI tool;
- inaccurate or harmful output that may have affected a pupil or another person;
- compromised AI account;
- safeguarding concern;
- discriminatory or inappropriate content;
- copyright concern; or
- unauthorised use of AI for school business.

Reports should be made to the Headteacher or designated AI lead and, where relevant, the DSL, Data Protection Officer or IT lead.

Failure to comply with this section or the Use of Artificial Intelligence Policy may be addressed under the school's disciplinary procedures. Any action taken will reflect the nature, seriousness and circumstances of the matter.

9. Monitoring, reporting concerns and consequences of unacceptable use

9.1 Monitoring of school systems

The school may monitor the use of its equipment, accounts, systems and networks for specified legitimate purposes, including:

- safeguarding pupils and staff;
- maintaining cyber security and system integrity;
- detecting malware, phishing, unauthorised access or data loss;
- managing the availability and performance of school systems;
- meeting legal and regulatory obligations;
- ensuring compliance with the school's Acceptable Use Agreement and relevant policies; and
- investigating reasonably suspected misconduct, safeguarding concerns, unlawful activity or serious misuse.

Monitoring will not be conducted merely because the technology makes it possible.

9.2 Data-protection requirements

Before monitoring is introduced or undertaken, the school will:

- clearly identify and document its purpose;
- identify an appropriate lawful basis and any additional condition required for special-category data;
- consider whether monitoring is necessary and proportionate;
- use the least intrusive method reasonably available;
- limit the information collected to what is necessary;
- define who may access the information and how it will be protected;
- establish an appropriate retention period;
- provide employees with clear and accessible privacy information; and
- consult the Data Protection Officer where appropriate.

A data-protection impact assessment will be completed where monitoring is likely to result in a high risk to individuals' rights and freedoms. Monitoring of the content of employees' emails or messages will be subject to a DPIA and will only take place where less intrusive monitoring would not achieve the identified purpose.

Information obtained through monitoring will not be used for an unrelated or incompatible purpose without an appropriate legal basis and further assessment.

9.3 Expectations of privacy

Employees should have a reasonable understanding that activity conducted through school-owned equipment, accounts, systems and networks may be recorded or monitored for the purposes described above.

This does not remove employees' rights to privacy. The school will have regard to applicable data-protection and human-rights requirements, including the right to respect for private and family life under Article 8 of the European Convention on Human Rights, as incorporated by the Human Rights Act 1998.

The school will not undertake indiscriminate or excessive monitoring. Particular care will be taken where monitoring could capture private communications, special-category data, communications with a trade union representative or information about individuals other than the employee.

9.4 Targeted and covert monitoring

Targeted monitoring may be considered where there is a specific and documented concern that cannot reasonably be addressed through a less intrusive method.

Covert monitoring will only be considered in exceptional circumstances, normally where:

- there are reasonable grounds to suspect criminal activity or conduct of comparable seriousness, such as potential gross misconduct;
- informing the employee in advance would be likely to prejudice the prevention or detection of that activity;
- senior management has authorised the monitoring;
- the Data Protection Officer has been consulted;
- a DPIA has been completed;
- the monitoring is strictly targeted, time-limited and proportionate; and
- the monitoring will end when the investigation is complete.

Covert monitoring will not normally be used in places where individuals have a particularly high expectation of privacy, such as toilets or changing rooms.

9.5 Reporting breaches of this policy

Employees who become aware of a suspected breach of this policy should report it promptly to the Headteacher or another appropriate senior leader.

Where the concern relates to the Headteacher, it should be reported to the Chair of Governors. Employees may also use the school's Whistleblowing Policy where appropriate.

Employees should preserve relevant evidence, such as messages, web addresses, usernames, dates, times or screenshots, where it is safe and lawful to do so. They must not conduct their own investigation, retaliate, increase the circulation of harmful material or attempt to conceal the matter.

9.6 Concerns about an adult's conduct towards a pupil

Any concern about an employee's, volunteer's, contractor's, governor's or other adult's interaction or communication with a pupil must be reported in accordance with the school's allegations against staff and low-level concerns procedures.

Such concerns should normally be reported without delay to the Headteacher, however small or uncertain the concern may appear. A concern about the Headteacher must be reported to the Chair of Governors.

A concern that a child may have been harmed or may otherwise require safeguarding support must also be brought immediately to the attention of the DSL or a deputy in accordance with the Safeguarding and Child Protection Policy.

If there is an immediate risk of harm, emergency services or children's social care should be contacted without delay.

9.7 Consequences of unacceptable use

A suspected breach of this policy will be considered fairly and proportionately, taking account of:

- the nature and seriousness of the conduct;
- whether the conduct was deliberate, reckless or accidental;
- any actual or potential harm;
- the employee's role and level of responsibility;
- any safeguarding, data-protection, equality or security implications;
- relevant mitigating circumstances; and
- consistency with the treatment of comparable cases.

A breach may result in:

- advice, support or additional training;
- restriction or removal of access to school systems;
- action under the school's disciplinary procedure;
- referral under safeguarding or allegations procedures;
- notification to the Data Protection Officer, local authority designated officer, Disclosure and Barring Service, Teaching Regulation Agency, Information Commissioner's Office or another relevant body where the applicable threshold is met; or
- referral to the police where criminal conduct is suspected.

Serious misuse may constitute gross misconduct and could result in dismissal without notice. A fair investigation and disciplinary procedure will be followed before any disciplinary decision is made.

Nothing in this policy prevents the school from taking immediate, proportionate steps to safeguard pupils, secure its systems, preserve evidence or prevent further harm while a matter is investigated.

10. Further information

Employees should normally seek advice through the school's internal procedures. Additional information is available from:

- Keeping Children Safe in Education;
- DfE online safety guidance for staff;
- ICO guidance on monitoring workers;
- UK Safer Internet Centre Professionals Online Safety Helpline; and
- Child Exploitation and Online Protection Safety Centre.

External sources of advice do not replace the school's safeguarding, data-breach, whistleblowing or emergency-reporting procedures.

11. Data protection

Personal information processed under this policy will be handled in accordance with the UK GDPR, the Data Protection Act 2018, the school's Data Protection Policy, applicable privacy information and the requirements set out in sections 6 and 9 of this policy.

Information will be collected only where necessary, kept secure, accessed only by authorised individuals, retained for no longer than required and disclosed only where there is a lawful basis to do so.

Any actual or suspected personal data breach must be reported immediately through the school's data-breach procedure. Employees must not decide independently whether the matter needs to be reported to the Information Commissioner's Office.

12. Roles, implementation and review

12.1 Governing body

The governing body is responsible for approving this policy and providing appropriate oversight of its implementation. It will seek assurance that appropriate safeguarding, employment, data-protection and cyber-security arrangements are in place.

12.2 Headteacher

The Headteacher has overall responsibility for implementing this policy, ensuring that it is communicated to employees and that concerns or suspected breaches are addressed under the appropriate school procedure.

12.3 Designated leads

The Designated Safeguarding Lead, Data Protection Officer, Online Safety Lead, designated AI lead and IT support will provide advice and carry out their respective responsibilities under this policy and the associated school policies.

12.4 Employees and other users

Employees and other people covered by this policy are responsible for:

- reading and following this policy and the relevant Acceptable Use Agreement;
- completing required training;
- maintaining appropriate professional boundaries;
- protecting school information, systems and accounts; and
- reporting safeguarding, data-protection, security or conduct concerns promptly.

12.5 Training and communication

The school will make this policy available to all employees. Relevant expectations will be included in induction and reinforced through safeguarding, online-safety, data-protection and cyber-security training and updates.

12.6 Monitoring and review

The Headteacher will review the implementation and effectiveness of this policy, taking account of reported incidents, changes in technology, identified risks and developments in legislation and statutory guidance.

The policy will be reviewed annually, or sooner where there is a significant legislative, safeguarding, technological or organisational change.