Social Media and Electronic Communications Policy

Policy Date:	September 2025		Author: Mr Steve Powell
Policy Review Date:	September 2026		
Ratified by Governing Body and Headteacher:			
Chair of Governors: Matthew Peatfield			Date: 01.09.25
Headteacher: Steve Powell			Date: 01.09.25

1. Introduction and scope

1.1 This policy forms part of the school's overall commitment to safety, wellbeing and duty of care at work. It applies to all employees at work but also off-duty if there is a detrimental effect to the school's reputation or the reputation of the employee themselves (i.e.in terms of how they may be viewed by the community the school serves) or impacts their ability to attend work or perform their duties.

1.2 This policy has been written to form part of the overall online safety framework. It is designed to complement the online safety policy and the acceptable use policy.

1.3 For the purposes of this policy, social media is any online platform or tool that allows users to create, share, or exchange information, opinions or content, including but not limited to, Facebook, X, LinkedIn, Instagram, and YouTube. Electronic communications are any form of communication that uses electronic devices or systems, including but not limited to, email, instant messaging, text messaging and video conferencing.

1.4 Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow this policy in relation to any social media used.

1.5 The use of the internet, electronic communication and social media sites has grown significantly and has vastly increased opportunities for teaching and learning. However, abuse of this technology, in terms of inappropriate use, has seen a significant increase in the number of disciplinary cases. This model policy is written to apply to all employees. The purpose of this policy is to ensure that:

- pupils and employees are safeguarded,
- the school is not exposed to legal risks,
- school employees have clear guidelines on what they can and cannot do to keep themselves safe and protected against allegations,
- teachers use of social media and electronic communications does not conflict with the national teacher standards,
- the reputation of the school is not adversely affected by inappropriate use,
- Heads are able to manage conduct effectively.

1.6 This policy should be read in conjunction with, and have due regard to, the following policies:

- Pay Policy
- Disciplinary Procedure
- Disciplinary Dismissal and Appeal Committee Hearings Procedure
- GDPR Data Protection Whole School Policy

1.7 This policy and procedure supports our obligation to work in line with current legislation, ACAS best practice, contractual requirements and national/local terms and conditions relevant to this area of employment practice.

1. Equalities and support

2.1 The Head will ensure that all reasonable adjustments or supportive measures are considered to allow equality of access and opportunity regardless of age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; or sexual orientation.

2.2 Through the implementation of this policy, the school will be mindful of the employer obligation to seek to maintain and protect the mental health and wellbeing of all staff as far as is reasonably practicable.

2.3 According to ACAS it is estimated one in seven people are neurodivergent, meaning that the brain functions, learns and processes information uniquely. Where an employee discloses neurodiversity, the school understands the employee may require extra support in relation to the application of this policy. Where reasonable adjustments are necessary and can be accommodated, the Head will support these.

2. Internet use

3.1 The internet is a valuable resource for teaching and learning. However, it can also present a high level of risk if it is abused or if safe practices are not adopted.

3.2 Employees are advised not to use school equipment to access the internet for private purposes unless they have express permission from the Head. The school network and use of the internet is closely monitored and individual usage can be traced - see paragraph 8 for further information. Inappropriate use of these facilities may constitute a disciplinary or criminal offence.

3.3 If employees or managers are unsure of what is or is not appropriate use of the internet, advice can be sought from the Online Safety Helpline by telephone on 0344 3814772 or by emailing helpline@saferinternet.org.uk.

3. Email use

4.1 Employees may only use approved email accounts on the school system.

4.2 What is written in an email may have to be released under data protection law. Employees therefore must not include information that may in any way breach data protection legislation or may cause embarrassment or offence (to the school or individuals). All communications must be professional and justifiable.

4.3 Employee to pupil email communication must only take place via a school email account or from within the learning platform.

4.4 Whilst emails are a valuable form of communication, unnecessary emails add to workload.

4.5 The following email use principles should be considered:-

Before sending an email consider;

- Is the email necessary?
- Is email the correct way to communicate the message?
- Is a reply required? If so, request a response.
- If sending or replying to a group email, does everyone need to receive the message?

When compiling an email ensure:

- To double check that the email has been addressed to the correct recipient(s).
- To include a clear and concise subject.
- That the email text is concise as possible.
- Large files are not included if sent internally – these could slow down the system so should be shared via Teams or OneDrive instead.

Always use a clear and concise subject. If the email concerns an individual, do not name them in the 'subject field'.

Employees should feel able to send emails when their working pattern suits them, however, they should not be required to read or respond to emails in the evenings or at weekends. They should respond to emails within 24 hours during their working week where a request for a response has been made. Part-time employees should use "out of office" automatic replies when they are not working.

Emails from parents should be responded to within 24 hours during their working week, unless in particular cases alternative advice has been given by their line manager or Headteacher. Excessive emails from parents should be raised with the line manager or Head.

4. Other internet-based communications

5.1 WhatsApp is an instant messaging mobile application which may be used by employees to communicate with their colleagues for either personal or work-related purposes.

5.2 Employees will consider the following when using internet-based communication methods:

- When communicating with colleagues on such platforms, ensure that they remain professional when discussing work related topics.
- Refrain from speaking about other employees in a negative manner.
- Refrain from making remarks that could be considered to constitute discrimination, harassment or abuse.
- Confidential information relating to other employees or pupils must not be discussed or shared on such platforms.
- Before sending an image, consider whether it is appropriate to send to another employee or to a group chat with other colleagues.
- Employees must not post illegal material in any work-based WhatsApp groups.

5.3 When using work based instant messaging platforms such as Microsoft Teams, employees must ensure that it is used only for professional communications relating to work. A professional tone must always be used and sensitive information must not be shared through chat.

5. Data protection, freedom of information and copyright

6.1 Employees should remain aware of their data protection and freedom of information obligations.

6.2 Personal data collected and processed during any monitoring exercise is in accordance with its data protection policy. Any data collected is held securely and accessed by or disclosed to individuals only for the purposes of completing the exercise or to comply with statutory obligations. Inappropriate access or disclosure of employee data constitutes a data breach and should be reported in accordance with the Data Protection Policy immediately. It may also constitute a disciplinary offence, which will be dealt with under the school's Disciplinary Procedure. Please also see paragraph 8 for further information regarding data protection and monitoring.

6.3 Employees should not copy and paste any images or text or make links to images on other sites on the internet, unless the other site specifically says that the images and/or text have been copyright cleared for use in that purpose.

6.4 Consideration should be given to what is being posted with regards to:

- is the information being posted in the public domain?
- if communicating through a web-based communication platform, is the platform secure?
- has permission been granted to publicise it from the person who created it?
- is the person who created it aware that the material is going to be made available on the internet?

6. Social media

7.1 Social media is part of many people's day to day lives. The following information has been put together to help employees understand what may be deemed appropriate or inappropriate, both inside and outside of work.

7.2 Communication via social media is rarely private. Employees should consider whether a comment would be said to a current or future colleague, parent, pupil or manager – if it would not, then it should not be published on a social media site, whether this is a school managed site or a personal one.

7.3 Online conduct should be as exemplary as offline conduct. Employees and volunteers must have regard to the fact that anything that is said on the internet could, at some point, be made public.

7.4 The school recognises that social media sites, websites and blogs provide a useful tool for communication and learning and are accessed widely. However, the safeguarding of pupils and employees is of paramount importance, adults should lead by example and set standards of behaviour. Therefore:

7.4.1 Safeguarding of pupils and employees is the responsibility of all employees and this should be taken into consideration when using personal social media sites inside and outside of the school. Employees should not link their own personal social media sites to anything related to the school and should not publicly indicate where they work or make their place of work publicly visible.

7.4.2 Employees are advised not to communicate with pupils or parents, nor should they accept pupils or parents as friends on social media sites using their personal systems and equipment. Where a member of staff is related to a pupil, the school should be made aware, if they are not already and consideration given to whether any safeguards need to be put in place. Employees should also carefully consider the implications of befriending parents, carers or ex-pupils as contacts on social media sites.

7.4.3 If employees use personal social media sites, they should not publish specific and detailed public thoughts or post anything that could bring the school into disrepute.

7.4.4 Where employees are members of social media groups or pages (e.g., Facebook groups), whether private or public, that refer to the school, any posts made in such groups should be in accordance with the school policies. This is particularly important where employee Facebook accounts are used principally for work purposes.

7.4.5 Employees must not place inappropriate photographs on any social media space and must ensure that background details (e.g., house number, street name, school) cannot identify personal/employment details about them.

7.4.6 Official blogs, microblogs (e.g., Twitter), sites or wikis run by staff or the school must be password protected and overseen and sanctioned by the school.

7.4.7 Contact should only be made with pupils for professional reasons via professional spaces set up and run by the school. If professional spaces are set up, steps should be taken to ensure the users of the space are not put at risk e.g., privacy settings, data protection and data security. Permission should be sought from the Head and the parents/guardians of pupils to communicate in this way.

7.4.8 Employees are advised not to run social media spaces for pupil use on a personal basis. If social media is used for supporting pupils with coursework, professional spaces should be created by employees and pupils as in paragraph 7.4.7 above.

7.4.9 Employees are advised not to use or access the social media sites of pupils, without due reason e.g., safeguarding purposes. However, this may not be possible to achieve if the situation in 7.4.2 applies.

8. Artificial intelligence

8.1 Artificial intelligence (AI) refers to computer systems that can think or act in a more human way, taking information from their surroundings to perform tasks that usually require human intelligence.

8.2 We understand the need to embrace emerging technology and recognise that AIpowered chatbots such as ChatGPT and Google Bard can produce impressive responses on a wide range of subjects. However, these large language models present a number of risks that cannot be ignored.

Risks associated with the use of AI

8.3 By the admission of the creators, AI such as ChatGPT, has its limits. For example, it can:

- give an incorrect answer to the question asked,
- give inconsistent answers when asked the same question more than once,
- provide outdated information,
- provide information that is biased or discriminatory,
- create a security or data protection risk when confidential information is inputted.

In addition, it can engineer a false view of someone's capabilities when the information it provides is used inappropriately.

Using AI

Because of the examples of risks given above, employees should exercise caution when using AI to carry out any aspect of their role.

Outside of working hours, employees must not input any information into AI that:

- identifies the school, either directly or indirectly,
- is reasonably considered to be confidential or sensitive information relating to the school

This is because AI learns from the information that is inputted and can provide information to subsequent users based on the information it receives.

Failure to comply with the above may result in disciplinary action being taken.

9. Monitoring and the consequences of improper/unacceptable use

9.1 Where it is believed unauthorised use of the information systems may be taking place, or the system may be being used for criminal purposes, then the decision may be taken to monitor the employee's use of the school's information systems e.g., email and/or internet use. Any monitoring will be conducted in accordance with a privacy impact assessment that the school has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the school's legitimate interests and is to ensure that this policy is being complied with. See paragraph 6 for more information on data protection.

9.2 Under data protection law, this type of monitoring is called 'occasional monitoring'. This is where the employer introduces monitoring as a short-term measure to address a particular issue e.g., performance or conduct, where concerns are of the nature explained above. Where monitoring takes place, the Governing Body must have due regard to article 8 of the European Convention on Human Rights, which means the employee still has a right to privacy in the workplace. This is the reason for the impact assessment, which should be carried out prior to any monitoring. Read the Employment Practice Guide on the Information Commissioner's Office (ICO) website, which provides an outline privacy impact assessment.

9.3 Employees must be aware that improper or unacceptable use of the internet or email systems could result in implementation of the Disciplinary Procedure and, in some cases, legal proceedings. Sanctions will depend upon the gravity of misuse and could result in summary dismissal in some cases.

9.4 This policy relies on employees acting responsibly and in accordance with the outlined restrictions. Where employees have concerns that a colleague is acting in breach of the outlined restrictions, they are encouraged to raise this with the Headteacher

9.5 If the concern involves possible inappropriate interaction between a colleague and a pupil, referral may be made to the designated safeguarding lead in the school.

10. Further information

- Child Exploitation and Online Protection (CEOP) website.

11. Data Protection

Personal data collected and processed for the purpose of this policy will be handled in accordance with the data protection policy and applicable statutory obligations. Any personal data collected is held securely and accessed by, and disclosed to, individuals only for the purposes of employee management or to comply with statutory reporting obligations. Inappropriate access to, or disclosure of, employee data constitutes a data breach and should be reported without delay, in accordance with the data protection policy. It may also constitute a disciplinary offence in which case it would be dealt with under the disciplinary policy and procedure.