



Internet, Social Media and Email Use Policy

Date: February 2021

Review date: February 2022

Approved by Advisory Board: February 2021

Linked with other policies:

- ICT and Internet Acceptable Use Policy
- Discipline guidelines on conduct for employees (Code of Conduct)
- Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings
- Anti-Bullying Policy
- Behaviour Towards Staff Policy and Procedures

Signed:

A handwritten signature in blue ink, appearing to read "S. Dagg".

1. Introduction

This policy has been written to form part of the school's overall online safety framework. It is designed to complement the school's ICT and Internet Acceptable Use Policy.

The use of the internet, emails 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 policy is written to apply to all employees in the school. The purpose of this policy is to ensure that:

- students 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 the internet, email and social media sites does not conflict with the national teacher standards,
- the reputation of the school is not adversely affected by inappropriate use,
- Headteachers are able to manage conduct effectively.

2. Equal Opportunities and Scope

The school expects employees and volunteers working in the school to adhere to this policy in line with the school's/academy's obligations under equality legislation. The Headteacher must ensure that all reasonable adjustments or supportive measures are considered to allow equality of access and opportunity regardless of age, gender, ethnicity, sexual orientation, disability, faith or religion, gender identity, pregnancy or marital status.

This policy should be read in conjunction with, and have due regard, to:

- ICT and Internet Acceptable Use Policy
- Discipline guidelines on conduct for employees (Code of Conduct)
- Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings
- The School's Anti-Bullying Policy

3. Internet use

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

Schools should advise employees not to use school equipment to access the internet for private purposes unless they have permission from the Headteacher. Employees should be made aware that the network and inappropriate use of the internet is closely monitored and individual usage can be traced - see paragraph 7 for further information. Inappropriate use of these facilities may constitute a criminal or disciplinary offence.

If employees or managers are unsure of what is or isn't appropriate use of the internet they can seek advice from the Online Safety Helpline by telephone on 0344 3814772 or by emailing helpline@saferinternet.org.uk.

4. Email use principles

- What is written in an email may have to be released under data protection law. Do not include information that may cause embarrassment, including to the school, maintain professionalism at all times.
- Always double-check that the email has been addressed to the correct recipient(s).
- If the e-mail concerns an individual, do not name them in the 'subject field'.
- Employee to student email communication must only take place via a school email account or from within the learning platform.
- Employees may only use approved e-mail accounts on the school system

5. Data protection, freedom of information and copyright

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

The school processes any personal data collected during any monitoring exercise in accordance with its data protection policy. Any data collected is held securely and accessed by, and disclosed to, individuals only for the purposes of completing the exercise. Inappropriate access or disclosure of employee data constitutes a data breach and should be reported in accordance with the school's 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 7 for further information regarding data protection and monitoring.

Employees should not copy and paste any images or text from 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.

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

- is the information being posted in the public domain?
- 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

Social media is the term commonly used for websites which allow people to interact with each other in some way (social networking) - by sharing information, opinions, knowledge and interests. Social media is part of many people's day to day lives. The following information has been put together for the benefit of employees to help them understand what may be deemed appropriate or inappropriate both inside and outside of work.

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

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.

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 students and

employees is of paramount importance, adults should lead by example and set standards of behaviour. Therefore:

6.1 Safeguarding of students and employees is the responsibility of all employees and this should also 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.

6.2 Employees are advised not to communicate with students or parents nor should they accept students or parents as friends on social media sites using their personal systems and equipment. Where a member of staff is related to a student 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 consider carefully the implications of befriending parents, carers or ex-students as contacts on social media sites.

6.3 Any communication with students should take place within clear and explicit boundaries.

6.4 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.

6.5 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's policies. This is particularly important where employee Facebook accounts are used principally for work purposes.

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

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

6.8 Contact should only be made with students 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 Headteacher and the parents/guardians of students to communicate in this way.

6.9 Employees are advised not to run social media spaces for student use on a personal basis. If social media is used for supporting students with coursework, professional spaces should be created by employees and students as in paragraph 6.7 above.

6.10 Employees are advised not to use or access the social media sites of students, without due reason e.g. safeguarding purposes. However, this may not be possible to achieve if the situation in 6.2 applies.

6.11 Cyberbullying of staff is not acceptable. The school has a separate policy for Cyberbullying. Please see this for what to do if this situation arises.

7. Monitoring and the consequences of improper/unacceptable use

7.1 Where the school believe 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 on email and internet use is being complied with. See paragraph 5 for more information on data protection.

7.2 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, schools 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.

7.3 Employees must be aware that improper or unacceptable use of the internet or email systems could result in the use of the school's 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.

7.4 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 or Chair of the Advisory Board/Directors if the concerns relate to the Headteacher.

7.5 If the concern involves possible inappropriate interaction between a colleague and a student, referral may be made to the designated senior professional in the school.

8. Further information

- Child exploitation and Online Protection (CEOP) website – internet safety