Caister
Primary Federation

Social media and electronic communications policy

Formally adopted by the Governing Board/ Trust of:-	**Caister Primary Federation**
On:-	**16th May 2024**
Chair of Governors/Trustees:-	**Payal Patel & David Wells**
Last updated:-	**July 2023**

Social media and electronic communications policy P319

Contents

(Click on the headings below to jump to the relevant section)

1. Introduction and scope 2
2. Equalities and support....3
3. Internet use 3
4. Email use....4
5. Other internet-based communications....5
6. Data protection, freedom of information and copyright....5
7. Social media....6
8. Artificial intelligence....7
9. Monitoring and the consequences of improper/unacceptable use....8
10. Further information 10
11. Data Protection....10

Appendix 1 – Table of changes 11

We, the Governing Board have adopted this policy and procedure.

1. Introduction and scope

1.1 This policy forms part of our 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 organisation'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 it 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 ICT code of conduct.

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,

- 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,
- Head of School s are able to manage conduct effectively.

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

- The Online Safety policy
- The ICT code of conduct
- The School Teachers' Pay and Conditions Document (professional duties and national conditions)
- *Discipline guidelines on conduct for employees G303c* on InfoSpace
- Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings
- *Discrimination, bullying and harassment policy P308* on InfoSpace
- The Cyberbullying 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.

2. Equalities and support

2.1 The Head of School 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 Governing Board/Trust 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 Governing Board/Trust 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 of School will support these.

3. 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 of School . The school network and use of the internet is closely monitored and individual usage can be traced - see paragraph 9 for further information. Inappropriate use of these facilities may constitute a disciplinary or criminal offence.

© 20XX Norfolk County Council

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.

4. 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 sending 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'.

When sending emails outside of the recipient's working hours, staff should be mindful of their colleagues and consider using the delayed send function, unless the content is deemed time sensitive/critical. Staff should not be expected to read or respond to emails in the evenings or on weekends. Emails should be responded to within 24 hours during their working days if a response is requested. Part-time employees could 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 Head of School . Excessive emails from parents should be raised with the line manager or Head of School .

© 20XX Norfolk County Council

"All staff" emails should be used sparingly and the staff bulletin or similar should be used as the main form of communication for non-sensitive information that needs to be distributed widely.

5. 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.

6. 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 *disciplinary procedure P303 (for schools) or P303a (for trusts)*. Please also see paragraph 9 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?

© 20XX Norfolk County Council

- 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?

7. 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 an employee 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 consider carefully 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's policies. This is particularly important where employee Facebook accounts are used principally for work purposes.

© 20XX Norfolk County Council

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. X), sites or wikis run by employees 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 of School 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.

7.5 Cyberbullying of employees is not acceptable. The school has a separate policy for Cyberbullying, which should be referred to if this situation arises.

8. Artificial intelligence

8.1 We understand the need to embrace emerging technology and recognise that AI-powered services such as ChatGPT and Google Gemini can produce impressive responses on a wide range of subjects. However, these large language models present a number of risks that cannot be ignored

8.2 It is not our intention to impose a ban on using AI-powered services to assist with work-related activities. In fact, we encourage their use where they can save time and expense.

8.3 Employees should be aware that the content inputted into an AI-powered services may be used to train its model and could form part of the responses to questions posed by other users.

8.4 Employees are strictly prohibited from sharing personal data and special categories of personal data with any AI-powered services, whether at work or in their own time

Personal data is any information that relates to a living individual who can be identified from that information.

Special categories of personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

© 20XX Norfolk County Council

Any personal data and special categories of personal data must be handled in accordance with our data protection policy/policy on processing special categories of personal data.

8.5 Employees are also prohibited from inputting any information (either at work or in their own time) which identifies their place or work, either the specific school or Trust (if applicable).

8.6 Failure to comply with any of 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 Board/Trust 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.

9.2.1 Systematic monitoring: E-safety monitors in schools, using an school email address, automatically receive a copy of any emails sent or received by school email accounts at the school which are flagged as a potential safety concern.

9.3 Where an incident, as described above occurs, the Head of School should contact their HR provider in the first instance to ensure that various legal requirements are adhered to.

9.4 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.

9.5 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 Head of School or Chair of Governors (or appropriate other role in an academy trust), if the concerns relate to the Head of School .

© 20XX Norfolk County Council

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

© 20XX Norfolk County Council

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.

© 20XX Norfolk County Council

Appendix 1 – Table of changes

Date of change	Paragraphs affected	Summary of update
23/10/2024	8.4, 8.5, 8.6	More detail added to AI use.
30/04/2024	All 8	Review of whole document and terminology to ensure consistency across all policies and procedures. Inclusion of artificial intelligence guidance
10/07/2023	All	Name of document changed and review of whole document, new paragraph inserted regarding internet-based communications. Paragraph 4 on email use expanded to include points from NEU protocol.
16/11/2021	2	Additional paragraph to include consideration for employees with mental health issues.
16/09/2020	All	All references to 'social networking changed to social media. Updated at 6.5 to state that where employees are members of social media groups that refer to the school, all post should be made in accordance with the school's policies
15/11/2018	Para 2 and 6.10	Updated to reflect the existence of the new model Cyberbullying policy.
17/05/2018	Para 5 and 7	Information added to take account of the General data protection regulations in force from 25 May 2018.
26/01/2018	Para 6.10	Updated to include further information about how to support staff who are victims of cyberbullying.
30/11/2017	Section 7 in the main	Section 7 updated to reflect that impact assessments should be undertaken prior to monitoring an employee and makes it clear that monitoring should only take place where it is a proportionate response to the issue. Whole policy also reviewed, this includes; updates references to non-HR documents and weblinks; reference to parents in para 6.2; reference to GDPR in para 5.
15/08/2017	6.11 (new para)	Information added to provide advice when a parent uses social media to write negative/defamatory comments about an employee(s).
01/03/2017	All	New formatting due to launch of new HR website, HR InfoSpace – no change to content

© 20XX Norfolk County Council