The Federation of Spixworth Schools

Internet, Social Media and Email Use Policy

This policy follows the model determined by Norfolk County Council.

Agreed by Governing Body: Autumn 2020
To be reviewed: Autumn 2021
Group Responsible: Full Governors

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

1. Introduction

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 model policy is written to apply to all employees in the federation. The purpose of this policy is to ensure that:

- pupils and employees are safeguarded
- the federation is not exposed to legal risks
- federation 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
- Head of Schools are able to manage conduct effectively

NB: To aid the federation in ensuring their online safety framework is robust and compliant related documents can be found on the Norfolk Schools website. Type ‘online safety’ into the search.

2. Equal Opportunities and Scope

The federation expects employees and volunteers working in the federation to adhere to this policy in line with the school’s obligations under equality legislation. The Head of School 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:

- The federation’s Online Safety policy
- The federation’s ICT code of conduct
- The School Teachers Pay and Conditions Document (professional duties and national conditions)
- Discipline guidelines on conduct for employees (G303e) on HR InfoSpace
- Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings
- The federation’s Dignity at Work or Bullying and Harassment policy
- The federation’s Cyberbullying policy

3. Internet use

The internet is a valuable resource for teaching and learning and is used regularly in schools. 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 Head of School. Employees

should be made aware that the network and inappropriate use of the internet is closely monitored and individual usage can be traced. Please 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 email: helpline@saferinternet.org.uk or call 0344 3814772.

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 federation, 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 pupil 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 federation 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 federation'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, pupil or manager then it should not be published on a social media site, whether this is a federation 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 federation 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:

6.1. Safeguarding of pupils 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 federation. Employees should not link their own personal social media sites to anything related to the federation.

6.2. 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 federation 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.

6.3. Any communication with pupils 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 federation 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 federation, any posts made in such groups should be in accordance with the federation's policies. This is particularly important where employee Facebook accounts are used principally for work purposes.

l

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 federation must be password protected and overseen and sanctioned by the federation.

6.8. Contact should only be made with pupils for professional reasons via professional spaces set up and run by the federation. 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.

6.9. 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 6.7 above.

6.10. 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 6.2 applies.

6.11. Cyberbullying of staff is not acceptable. The federation 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 federation 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 federation's information systems e.g. email and/or internet use. Any monitoring will be conducted in accordance with a privacy impact assessment that the federation has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the federation's legitimate interests and is to ensure that this policy on email and internet use is being complied with. Please also 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 both 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. The ICO's employment practices guide provides an outline privacy impact assessment on page 59-64 of its guidance.

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

7.3. Where an incident, as described above, occurs the federation should contact Educator Solutions HR Services in the first instance. This is to ensure that various legal requirements are adhered to.

7.4. Employees must be aware that improper or unacceptable use of the internet or email systems could result in the use of the federation'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.

7.5 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 Executive Headteacher if the concerns relate to the Head of School.

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

8. Further information

- Child exploitation and Online Protection (CEOP) website – internet safety
- Educator Solutions HR Services (01603 307760 or HRenquiry@educatorsolutions.org.uk)

Appendix 1 – Table of changes

Date of change	Paragraphs affected	Summary of update
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