# The Swallowtail Federation of Church Schools

# Internet, social networking and email use Policy

**(Feb 18 – to be formally agreed by Govs in March 18)**

| Formally adopted by the Governing Body | Swallowtail Federation |
|---|---|
| On:- | |
| Chair of Governors | Sheila Watts |
| Last updated:- | |

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

This model has been agreed by recognised trade unions for schools and academies at County level.

## 1. Introduction

This model policy has been written to form part of the school's overall online safety framework. It is designed to complement the school's online safety policy and the ICT code of conduct.

The use of the internet, emails and social networking 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 school. 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 the internet, email and social networking 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

**NB**: To aid the school 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 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:

- The school's Online Safety policy
- The school'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

### 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. 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 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 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. See the GDPR pages of HR InfoSpace regarding data protection requirements.

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 networking

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 networking 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 networking 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 networking sites inside and outside of the school. Employees should not link their own personal social networking sites to anything related to the school.

6.2.    Employees are advised not to communicate with pupils or parents nor should they accept pupils or parents as friends on social network 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 consider carefully the implications of befriending parents, carers or ex-pupils as contacts on social networking sites.

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

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

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

6.6. 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.

6.7. 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 Headteacher and the parents/guardians of pupils to communicate in this way.

6.8. Employees are advised not to run social network spaces for pupil use on a personal basis. If social networking is used for supporting pupils with coursework, professional spaces should be created by employees and pupils as in paragraph 6.7 above.

6.9. Employees are advised not to use or access the social networking 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.

6.10. Cyberbullying of staff is not acceptable. If an employee feels they are a victim of cyberbullying they should do the following:

- Never respond or retaliate. Report it via the appropriate channels and seek support from the Headteacher or a senior member of staff
- If possible, save evidence of the abuse – screen shots and record the time and date
- If the comments are threatening, abusive, sexist of a sexual nature or constitute a hate crime consider calling the police.

If employees or managers need to seek advice about inappropriate use they can contact the Online Safety Helpline (email: helpline@saferinternet.org.uk or call 0344 3814772). However, employees and managers should not bypass the school's safeguarding procedures.

6.10.1 If a parent/guardian makes inappropriate comments about a member of staff on social media the school should take appropriate action. As a first step the employee(s) in question should be offered support as the situation is likely to cause distress. They should be advised not to respond to the post(s) on social media. Additionally, the school should have a discussion with the parent, which could include advice on available routes for concerns; discussion of a resolution to the concern and request to remove the information. Further steps could potentially include taking legal advice if the information is defamatory or contact with the Police if there are grounds for harassment.

Click here for DfE guidance on Cyberbullying and school staff.

## 7. Monitoring and the consequences of improper/unacceptable use
7.1. A school or academy can exercise their right to monitor an employee's use of the school's information systems and internet access. Monitoring will take place where

the school believe unauthorised use of the information system may be taking place, or the system may be being used for criminal purposes, or for storing unauthorised text, imagery or sound. This policy informs employees of what monitoring may take place and the reasons for it.

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

7.3. 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. Therefore, the school should carry out an impact assessment before undertaking any monitoring. This will help to determine whether monitoring is a proportionate response to the issue and therefore lawful. The ICO's employment practices guide provides an outline impact assessment on page 59-64 of its guidance.

7.3.1. 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 school which are flagged as a potential safety concern. Academies may have different automatic monitoring in place. For advice regarding this type of monitoring please speak with the school/academy's ICT provider.

7.4. 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.

7.3 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 Governors if the concerns relate to the Headteacher.

7.4 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.

## 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 |
|---|---|---|
| 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 |