



# **Social Media Policy**

Fenstanton and Hilton Primary School

Reviewed By: The Full Governing Body

Date of Review: May 2026

Date of Next Review: May 2027

Version: 1.0

## Policy Version Control

Date	Version	Amendments/Comments	Reviewer/s
06.05.26	1.0	Initial version	FGB

## **Policy adopted from the ICT Service model**

### **Objectives:**

This policy sets out Fenstanton & Hilton Primary School policy on social networking. Social networking activities conducted online outside work, such as blogging, involvement in any social networking sites such as Facebook or Twitter and posting material, images or comments on sites such as YouTube can have a negative effect on an organisation's reputation or image.

In addition, Fenstanton & Hilton Primary School has a firm commitment to safeguarding children in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff, with respect to their responsibilities in connection with the use of social networking sites.

### **Key Principles**

- Everyone at Fenstanton & Hilton Primary School has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.
- It is important to protect everyone at Fenstanton & Hilton Primary School from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is paramount and is a key responsibility of all members of staff and it is essential that everyone at Fenstanton & Hilton Primary School considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.
- With safeguarding in mind, staff, parents, pupils and visitors are prohibited from using mobile phones in public areas around school and on school premises.
- This policy relates to social networking outside work. Blogging and accessing social networking sites at work or at home using school equipment is not permitted, unless for professional purposes and authorised by the Headteacher.
- It is also completely unacceptable to communicate on social media about the school or any member of the school community in or out of work on personally owned equipment.

### **Aims**

- To set out the key principles and code of conduct expected of all members of staff, governors, friends and volunteers at Fenstanton & Hilton Primary School with respect to social networking.
- To further safeguard and protect children and staff.

## **Overview and Expectations**

All adults working with children have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children, public in general and all those with whom they work.

Adults in contact with children should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting. The guidance contained in this policy is an attempt to identify what behaviours are expected of the school's staff who work with children.

Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

## **Code of Conduct: Social Networking**

**Under no circumstances should staff make reference to any staff member, pupil, parent or school activity/event.**

The following are also **not considered acceptable** at Fenstanton & Hilton Primary School:

- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

**In addition to the above everyone at Fenstanton & Hilton Primary School must ensure that they:**

- Communicate with children and parents in an open and transparent way using the school phone number and email address.
- Never 'friend' a pupil at the school where they are working onto their social networking site.
- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings.

- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- Make sure that high levels of privacy are set if they choose to use social media.
- Enforce the expectation that mobile phones must not be used on the premises by parents and carers.

### **Potential and Actual Breaches of the Code of Conduct**

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure.
- A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.
- The Governing Body will take appropriate action to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Headteacher of the justification for any such action already taken or proposed. The Headteacher will in turn seek advice from Education Personnel Management (the school's HR provider) where appropriate. This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation.

### **Safer Online Behaviour**

Some social networking sites and other web-based sites have fields in the user profile for job title etc.

**If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the local authority.**

In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for children or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties. All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, children or other individuals connected with the school, or another school, or the Local Authority could result in formal action being taken against them. This includes the uploading of photographs which might put the school into disrepute.

## **Mobile Phones/Camera/Video Recorder Usage**

**To ensure the safety and welfare of children in our care, personal mobile phones, cameras and video recorders must not be used when children are present.**

- All mobile phones must be kept in a secure place (not in a pocket) and not accessed throughout contact time with the children.
- In exceptional circumstances, which have been discussed and agreed with a member of the leadership team, staff may keep their phone switched on and accessible as long as they use their phone out of view of children, i.e. in a room designated for staff, e.g. the staff room or school office.
- During school visits mobile phones should be used away from the children and for emergency purposes only.
- Photographs or images of any children within our care may only be taken following parental consent and only using one of the school cameras / Ipads. These images should remain within this setting or be shared only with the parents of the child concerned.
- Personal mobiles, cameras or video recorders cannot be used to record classroom activities. ONLY school property can be used for this.
- School photographs and recordings can only be transferred to and stored on a school computer.

## **Protection of Personal Information**

Staff should not give their personal email addresses to children or parents. Where there is a need for communication to be sent electronically the school email address should be used. Likewise, staff should keep their personal phone numbers private and not use their own mobile phones to contact children or parents in a professional capacity. There will be occasions when there are social contacts between children and staff, where for example the parent and teacher are part of the same social circle or members of the same parish or community. These contacts, however, will be easily recognised and openly acknowledged. Staff have a responsibility to make any such contact known to the senior leadership team. Staff should never share their work log-ins or passwords with other people.

## **Access to Inappropriate Images and Internet Usage**

There are no circumstances that will justify adults possessing indecent images of children. Staff accessing and possessing links to such websites will be viewed as a potential and significant threat to children. Accessing, making and storing indecent images of children are illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven. Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Where indecent images of children are found by staff, the police should be immediately informed. Schools should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which can lead to a criminal prosecution. Where other unsuitable material is found, which may not be illegal, but which raises concerns about that member of staff, the Headteacher (and in the Head's absence, a member of the SLT) should be informed and that person will seek advice from their HR representative. The school will not attempt to investigate or evaluate the material themselves until such advice is received.

## **Cyber-bullying**

Fenstanton & Hilton Primary School's definition of cyber-bullying is 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

In order to reduce the potential for cyber-bullying, children are not allowed to bring phones into school. If a mobile phone is brought into school by a child, it must be kept in the main office until home-time and parents made aware.

Prevention activities are key to ensuring that staff are protected from the potential threat of cyber-bullying. All employees are reminded of the need to protect themselves from the potential threat of cyber-bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

If cyber-bullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or emails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

Staff are encouraged to report all incidents of cyber-bullying to their line manager or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

## **Link with Other Policies**

This policy should be read in conjunction with the following school policies: All School information, data-related, IT and IT safety policies

Safeguarding (Child Protection) Policy

Whistle-blowing Policy

All employees must adhere to, and apply the principles of the policy in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

## **Review of Policy**

Due to the ever-changing nature of information and communication technologies it is best practice that this policy be reviewed annually. Refer to the front cover for the latest version.