



Kilby St Mary's C of E (Aided) Primary School

Social Media Policy & Guidelines

Date:	May 2025
Signed:	<i>RP J-O'Reilly</i> <hr/>
Name & Position:	The Reverend Canon Philip O'Reilly, Chair of Governors
Review By:	May 2028

Contents

Section	Content
1	Purpose
2	What is Social Media
3	The Use of Social Media
4	Employee Responsibilities
5	Disciplinary Action
6	Social Media Security
7	Monitoring the Use of Social Media Websites
8	
9	
10	
11	
12	
13	
14	

This guidance applies to all staff, including Head Teachers / Principals, Teachers and all Support Staff regardless of whether they are permanent, fixed term, casual or agency or volunteers. It provides guidance on what measures are to be taken to ensure the safe use of social media and defines what is considered to be inappropriate conduct when using social media/internet sites for both professional and personal purposes.

Breaches of this guidance may be dealt with via the schools disciplinary policy or where it is appropriate will be referred to the police.

For the purposes of this guidance Head teachers/Principals will be referred to as Head teacher and School/Academy will be referred to as school.

Documents to support this Guidance:

In addition, this Guidance should also be read in conjunction with the school's handbook/code of conduct/e-comms /e-safety / title of schools own Guidance(s) (or equivalent)] Guidance.

In addition schools should also take account of any current and relevant legislation.

1. Purpose

The primary purpose of this guidance is to clarify how all employees should conduct themselves when using all forms of social media whether this is done through the school's media or personal media, in work time or in an individual's own time. The aim being to minimise the risk employees may place themselves and pupils in when they choose to write about their work or matters relating to the school and/or their personal lives.

This in turn will minimise situations where safeguarding concerns could arise, employees' integrity or professional standing could be undermined, professional relationships with colleagues and pupils are compromised or the school [and / or the Local Authority (for Maintained Schools)] brought into disrepute. Additionally, adhering to the Guidance reduces the risk of employees inadvertently contravening sections of the Data Protection Act or falling foul of any breaches of confidentiality, privacy, libel, defamation, harassment and copyright laws.

Whilst this Guidance is not intended to prevent employees from using social media sites, it does aim to make employees aware of the risks they could face whilst doing so and highlight what is deemed to be unacceptable when sharing information about their professional and/or personal life. Employees should be encouraged to report any concerns that they have regarding content placed by employees on social media sites to the Head teacher.

When an employee(s) wishes to create a work-related social media site they must discuss this with and obtain the relevant approval from the Head teacher. Creators of these groups are responsible for monitoring the content of the site and ensuring that it is appropriate and not in breach of any of the terms in this Guidance.

Application of the Guidance

The Social Media Guidance will be managed by either the Head Teacher or another manager. If the matters are regarding the Head Teacher, then the Chair of Governors will be responsible for overseeing this Guidance.

2. What is Social Media?

For the purposes of this Guidance, the term social media is used to describe a type of interactive website or online tool that allows parties to communicate or interact with each other in some way by sharing information, opinions, knowledge and interests and to share data in a public forum or to participate in social networking, resulting in a number of different activities.

Social Media activities include, but are not limited to:

- Maintaining a profile page on social / business networking sites such as Facebook, Twitter, WhatsApp or LinkedIn
- Writing or commenting on a blog, whether it is your own or the blog of another person/informational site.
- Taking part in discussions on web forums or message boards such as YouTube.
- Leaving product or service reviews on business websites or customer review websites.
- Taking part in online polls.
- Uploading multimedia on networking sites such as You Tube, Instagram, WhatsApp Twitter and Tumblr.
- Liking, re-tweeting and commenting on posts of your own, another person or other social media account.

Many other forms of social media also exist which are not listed in this Guidance. Employees need to be aware that this area is constantly changing and they are reminded of their continued responsibility to keep

up to date with developments and review their privacy settings on a regular basis when using social media sites.

3. The Use of Social Media

The school recognises that employees will use social media in a personal capacity. However, it is important that employees understand that they are personally responsible for all comments, images or information that they post online. Therefore all employees must ensure that when posting any information, images or making comments, they do not:

- **Bring the School into disrepute.** E.g. by making derogatory or defamatory comments, either directly or indirectly, about the school, colleagues, individuals, pupils or parents etc that could negatively impact on the schools reputation or cause embarrassment. This includes posting images or links to inappropriate content or using inappropriate language.
- **Breach confidentiality.** E.g, revealing confidential information owned by the school relating to its activities, finances, employees or pupils.
- **Undertake any behaviour which may be considered discriminatory, or as bullying and/or harassment of any individual.** E.g, making offensive or derogatory comments (either directly or indirectly) relating to sex, gender, race, disability, sexual orientation, religion, belief or age; using social media to bully (“Cyberbullying”) another individual; or posting images that are discriminatory or offensive or linking to such content.

As with all personal internet use, employees using social media sites must also observe the specific requirements of the documents named at the beginning of this policy.

4. Employee Responsibilities

Employees are personally responsible for the content that they publish on social media sites, including “Likes” (on Facebook) / “re-tweets” (on Twitter), Snapchat, Instagram, LinkedIn, Yammer, WhatsApp etc. Employees should assume that everything that is written is permanent and can be viewed by anyone at any time. It is fair and reasonable to take disciplinary action against employees for inappropriate use of social media, including use of social media conducted outside of working hours.

Employees must observe and note the following listed guidance (which is not exhaustive).

- Employees should assume that everything can be traced back to them personally as well as to their colleagues, the school, pupils and parents.
- To avoid any conflict of interest, employees must ensure that personal social networking sites are set to private and pupils are never listed as approved contacts. An exception to this may be if the child is the employee’s own child, relative, or family friend.
- Information must not be posted that would disclose the identity of pupils or could in any way be linked to a pupil(s). This includes photographs or videos of pupils or their homes.

- Pupils must not be discussed on social media sites.
- Employees should not post information on sites including photographs and videos that could bring the School [or the Local Authority] into disrepute.
- Employees must not represent their own views/opinions as being those of the school [or the Local Authority].
- Employees must not divulge any information that is confidential to the school [the Local Authority] or a partner organisation.
- Potentially false, derogatory, offensive or defamatory remarks directly or indirectly towards the School, [the Local Authority], employees, pupils, pupils' relatives, the school [or Local Authority] suppliers and partner organisations should not be posted on social media sites.
- Employees must ensure content or links to other content does not interfere with their work commitments, or be on an inappropriate content.
- Employees must not either endorse or criticise service providers used by the school [or the Local Authority] or develop on-line relationships which create a conflict of interest.
- Employees must not upload, post, forward or post a link to any pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature).
- When posting on social media sites employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive, obscene, derogatory, discriminatory language which may also cause embarrassment to school the Local Authority, employees, pupils, pupils' relatives, Council suppliers and partner organisations.
- Employees must never impersonate another person.
- Employees must not upload, forward or post a link which is likely to: create any liability for the School (whether criminal or civil), breach copyright law or other affect intellectual property rights, or which invades the privacy of any person.

Think before you post. There is no such thing as a private social media site. Social networking platforms/ Chat Rooms and discussion forums etc are in the public domain and it is not always possible to be sure what is being viewed, shared or archived, even if material is posted on a closed profile or group. There can be no reasonable expectation that posts will remain private and will not be passed on to other people, intentionally or otherwise.

5. Disciplinary Action

Employees should be aware that the use of social media sites in a manner contrary to this guidance, including if others implicate you in a breach of any of the points listed within this document may result in disciplinary action and in serious cases may be treated as gross misconduct, which itself could lead to summary dismissal.

In certain circumstances, such misuse may constitute a criminal offence or otherwise give rise to legal liability against employees and the school. Such cases will be referred to the police (and, where necessary the nominated safeguarding lead at the County Council) to investigate further.

Employees who become aware of any use of social media by other members of staff in breach of this guidance must report the matter to the Head teacher.

6. Social Media Security

Employees should be mindful when placing information on social media sites that this information is visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for identify fraud, false allegations and threats. In addition it may be possible through social media sites for children or vulnerable adults to be identified, which could have implications for their security. Employees should therefore be mindful that they:

- Do not reveal personal or private information about themselves such as date of birth, address details and bank details etc. Posting such information could increase the risk of identity theft.
- Remember that there is the scope for causing offence or unintentionally causing embarrassment, for example if pupils find photographs of their teacher which may cause embarrassment and/or damage to professional reputation and that of the School.
- Be mindful that posting images, comments or joining on line campaigns may be viewed by colleagues, parents, ex-pupils etc.
- Ensure that where you do post comments make a clear statement that any comments expressed are your own and not those of the school [or Local Authority].

Finally, consideration should be given to the information posted on social media sites and employees are advised to use appropriately the security settings on such sites in order to assist in limiting the concerns above.

7. Monitoring the Use of Social Media Websites

Employees should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this Guidance are found, action may be taken under the Disciplinary policy.

The School considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been using social media websites when he/she should be working; or
- acted in a way that is in breach of the rules set out in this Guidance.