

Grange Primary School



Grange Primary School
Pursuing excellence for every child

Social Media Policy

Review Date: March 2026

Grange Primary School

Social Media Policy

Grange Primary School recognises the importance of the Internet and mobile communications technology in shaping public and internal thinking about the school.

The school also recognises the value to our staff in joining in and helping shape educational direction through blogging and interaction in social media. We are committed to supporting rights to interact responsibly, knowledgeably and socially on the Internet through email, blogging and communication in social media so that the confidentiality of pupils, staff and the reputation of the school are safeguarded.

Purpose of the Policy

1. To minimise the reputational, legal and governance risk to the school and its employees, arising from use of social media by staff in personal and professional capacities.
2. To enable the safe use of social media for the purposes of communication and engagement.
3. To ensure a consistent approach is applied across the school

We are also committed to ensuring that all staff employed by the school are aware of their vulnerability to identity theft and the potential threat to their profile and professional standing by posting inappropriate personal information on the internet via social networking sites thus leaving an "electronic footprint", compromising themselves and/or Grange Primary School.

It's not just a matter of personal safety. What seems frivolous or even trivial to you in a friendship group could damage your reputation when seen by others. For example, pictures taken at parties and posted on a profile can cause embarrassment, or worse, when seen by parents, colleagues and employers. Before you post something, ask yourself what impression someone would get from seeing your web presence? Can this be linked back to my place of work and cause embarrassment or damage my professional role and /or Grange Primary School?

This policy makes clear to all staff the steps necessary to protect themselves and the school in making appropriate decisions about what content is suitable to post on social media, or other such websites where comments can be seen both publicly and privately.

The schools Computing policy and online safety Policy remains in effect.

Please note that this policy applies only to online content that has a direct or indirect connection or link to Grange Primary School or that may be inferred as being the opinion of Grange Primary School. The policy does not infringe upon your personal interaction or

commentary online unless the contents of such interaction or commentary are seen as a breach of professional trust between you and Grange Primary School.

Interaction on the Internet and via mobile communication technology

- The Professional expectations of confidentiality regarding the day-to-day functions, practices and events that happen within Grange Primary School do not change when using the internet or mobile communication technology. Staff are expected to speak respectfully about the school and our current and potential employees, students, and partners. Do not engage in 'name calling' or behaviour that will reflect negatively on the school's reputation. Note that the use of unfounded or derogatory statements or misrepresentation is not viewed favourably and may result in formal disciplinary action. Unless given permission by your manager, you are not authorised to speak on behalf of the School, or to represent that you do so.
- Staff members must not identify themselves as employees of Grange Primary School. This is to prevent information on these sites from being linked with the school and safeguard the privacy of staff members.
- If, through existing friendship, staff have social media connections with pupils' family members, caution should be exercised to ensure that the integrity of the staff member and the school are maintained at all times.
- Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts.
- Information that staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues and other parties must not be discussed on their social media platforms.
- Any online presence should not make reference to Grange Primary School for example you are not authorised to utilise your school email address when joining social networking sites or making the school supplied email address your primary method of contact.
- The Grange Primary School logo and name may not be used without explicit permission in writing from the Head teacher. This is to prevent the appearance that you speak for or represent the company officially.
- Photographs, videos or any images of pupils should not be published on personal social media platforms without prior permission of parents/carers and the school. Permission should be gained through existing school procedures and conforms with the expectations of GDPR. Ensure that the school policy on displaying pupil images and information is adhered to.
- Recognise that staff are legally liable for anything they write or present online. Staff may be formally disciplined by the school for commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. You may also become the subject of litigation by colleagues, and any individual or company that views your commentary, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. Liability can arise under the laws of:

- Defamation
- Copyright
- Discrimination
- Contract
- Human Rights
- Protection from harassment
- Criminal Justice
- Data Protection

Caution is advised when inviting work colleagues to be 'friends' in personal, social networking sites as it can blur the line between work and personal lives' and it may be difficult to maintain professional relationships.

Staff members must ensure the privacy levels of their personal sites are as strictly as they can and strongly advised to opt out of public listings to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so any other personal details are given away. This needs to be adhered to under the new GDPR guidelines.

Staff should also select carefully their social media profile picture as it is and extension to their professional image online.

Social media should not be used for work related communication. Communication should be through school email or contact details held by the school.

Honour the privacy rights of your colleagues by seeking their permission before writing about or displaying internal school events that might be considered to be a breach of their privacy, confidentiality and a breach of General Data Protection Regulations recognise that as a member of staff of Grange Primary School your online opinions, interactions and internet presence are influential to the young people that we support and as such should always be balanced and appropriate so that no inference of political, sexual or racist bias can be construed. Staff must at all times act in the best interests of the school and its pupils when creating, participating in or contributing content to social media sites.

Where a member of staff is a parent/carer as well as an employee of the school.

Use professional judgement (in reference to child protection and safeguarding policies) when communicating with children also connected to the school community.

Access to social media sites for personal reasons is not allowed between 8:30am and 4pm.

The above points are not exhaustive and only cover a range of what Grange Primary School

considers confidential and proprietary. If you have any questions about the appropriateness of online information released publicly or doubts of any kind, please speak to the Computing Leader or a member of the senior management team before releasing information that could potentially harm our school, or our staff, students, and school community.

Monitoring

All school systems may be monitored in accordance with the Acceptable Use Policy, so personal privacy cannot be assumed when using school hardware.

The school can monitor the usage of its own internet and email services when justifiable concerns have been raised in line with the school's procedures.

Publically accessible postings may be investigated if there is a suspected breach of this or related policies.

When a public post is reported concerning non-employee members of the school community, this will be investigated and responded to by the school.

Any misuse or abuse of social media must be reported to the Head Teacher as soon as noticed, especially when concerning a pupil, parent/carer or employee.

Date ratified by the Governing Body: March 2025

Date last reviewed: Feb 2025

Next review date: March 2026

Signed Virtually by Chair of Governors: *Mr S. Ryley* **Date:** March 2025