LORDSWOOD SCHOOL

School Social Networking Policy

Date: March 2026
Review Due: March 2027
Reviewed Annually

Introduction

This policy should be read in conjunction with other relevant policies e.g. Computing and ICT Policy and Online Safety.

All staff stakeholders at the school need to be aware of the risks and accountability of inappropriate or inadvertent provision of information about themselves, the school, its pupils and staff or the wider school community in the Social Media arena.

Every employee or volunteer working within the school setting is accountable for information published and must be aware that such information may be monitored by the Head or their representative.

It is important to note that information available in the public domain which has the potential for harm, distress or reputational damage may lead to disciplinary action being taken.

What is Social Networking and Social Media?

Social networking and social media are communication tools based on websites or networks which allow you to share information or other material about yourself and your interests with groups of other people. These groups of people could be:

- People who are known to you (friends or colleagues)
- People you don't know but who share common interests (such as Teaching, working, ADHD etc)
- Anyone who could find your comments through search engines.

Examples of Social Media and Social Networking sites and services include (but are not limited to):

- Facebook
- Instagram
- WhatsApp
- Twitter
- YouTube
- LinkedIn
- Blogs
- discussion groups
- mailing lists

What social media activity does this policy cover?

This policy is mainly concerned about two types of Social Media activity:

- Your own personal activity, done for your friends and contacts, but not under or in the name of Lordswood School (or The Griffin School's Trust).
- Activity carried out in the name of Lordswood School, such as a school website, Twitter posting or a Facebook Group that represents, or appears to represent, the official views of the school.

This policy is not about stopping you using or accessing such groups, but aims to ensure that your use of social media does not harm the interests of the children and young people we support, or damages the reputation of the school, Trust or school staff. Adherence with the good practice guidelines in this document will help protect you against posting things that you might regret or may harm you later.

Aim of this policy

This policy recognises that new technologies are an integral and growing part of everyday life and make an important contribution to teaching and learning opportunities. However, the rapid evolution of social networking technologies requires a robust policy framework and this policy aims to:

- Assist staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with children
- Prevent adults abusing or misusing their position of trust.

This document applies to all staff who work in the school whether paid or unpaid. This includes members of the Governing Body, whether Parent, Community or Trust Governors.

Principles

The principles that underpin this policy are:

- Adults who work with children are responsible for their own actions and behaviour and must avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Adults in the school must work and be seen to work, in an open and transparent way.
- Adults in the school must continually monitor and review their own practice in terms of the continually evolving world of social networking and ensure that they consistently follow the guidance contained in this document.

Why do we need the policy?

There have been numerous examples of people in all walks of life posting things on social media that they have later regretted, because that information has harmed or put at risk themselves or others. This includes:

- Accidentally posting personal or embarrassing information about themselves or others in a public forum or beyond the group the information was originally intended for.
- Sharing information about yourself or others with people you don't know that could be used by someone to commit fraud or misrepresent the views of yourself or others (such as identity theft)
- Breaching privacy or child protection laws and regulations or workplace policies by posting information about your work or the children and adults that you work with
- You or others receiving negative publicity, harassment, inappropriate contact or threats as a result of your views, beliefs or comments.

This has led to people facing disciplinary action, losing their jobs, being prosecuted or even imprisoned.

This policy and guidance will help to make sure that your use of social networking sites and social media is safe.

Safer Social Networking Practice

This document applies to current social networking sites such as Facebook, Instagram, Twitter etc and all other current and emerging technologies.

The Safer Social Networking Practice is broken down into:

- Things you must not do, because they are illegal, contrary to regulations or against school policy (such as professional boundaries)
- Things you should do to avoid risk to yourself or others
- Good Practice, things you should do to reduce the risk that information you put on social networking sites or media cannot later be used against you

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

Social Networking "Must Nots"

- Staff or volunteers must not make comments on behalf of the school or claim to represent the views of the school, unless they have explicit permission to do so.
- Staff or volunteers should never make a 'friend' of a pupil at the school where they are working on their social networking page and seek the advice from the Head or Assistant Head before becoming 'friends' with ex-students.
- Staff or volunteers should not make a "friend" of a parent/carer of a pupil at the school, and should seek advice from the Head or Assistant Head before making a "friend" of the parent/carer.
- Staff or volunteers should never use or access social networking pages of pupils.
- Staff or volunteers must not request, or respond to, any personal information from a pupil.
- Staff or volunteers should never post confidential information about themselves, the school, the governing body, the Trust, their colleagues, pupils. If they are posting in an "official" capacity, they should not post confidential information about members of the public.
- Staff and volunteers should not make allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or the Trust. Doing so may result in disciplinary action being taken against them. If they have concerns about practices within the school or the actions of pupils or parents, they most act in accordance with the school's Whistle-Blowing Policy.
- E-mail or text communications between a staff member/volunteer and a pupil outside must not take place outside of agreed protocols.

Social Networking "Shoulds"

- All adults, particularly those new to the school setting, 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/or the school if they were to be published outside of the site.
- Adults within school settings need to be aware of the dangers of putting their personal information onto social networking sites such as addresses, home or mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside the school environment. It also reduces the potential for identity theft by third parties.
- Some social networking sites and other web-based sites have fields in the user profile for job title etc. As an employee or volunteer of the school and particularly if you are a teacher or

teaching assistant, 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 and the profession. If it is a work-based site where you are required to provide this information, you must obtain the permission of the Head beforehand.

- Staff and volunteers should keep their personal phone numbers, work login or passwords and personal email addresses private and secure. Where there is a need to contact pupils or parents the school email address and/or telephone should be used. If, with permission, telephone calls are made from a personal phone (landline or mobile phone) the telephone number the call is being made from must be withheld when making calls by prefixing the dialled number with 141.
- Staff and volunteers should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils in order to avoid any possible misinterpretation of their motives or any behaviour which could possibly be construed as 'grooming' in the context of sexual offending.
- E-mail or text communications between a member or staff or volunteer and a pupil should only take place within agreed protocols and for email within the confines of the Acceptable Use Policy.
- There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged with the Head where there may be implications for the adult and their position within the school setting.

Posting on behalf of the School

Staff members are not permitted to post on behalf of the school without specific permission, which will apply to specific sites.

For example, the Head may give permission for staff to post as teachers at Lordswood School in specific discussion groups related to working with pupils with ADHD. In such cases, the Head will make it clear the capacity in which the person may post and the scope and subject of their postings.

Social Networking Good Practice

Staff and volunteers must understand who is allowed to view the content on their pages of any sites they use and how to restrict access to certain groups of people.

- On Facebook, they should understand whether the posts they make are Public (which means that anyone can see them), visible to Friends (which means that only people on their Friends list can see them) or visible to Friends of Friends, which means that the posts are visible to all the friends of their friends, which could be many hundreds or even thousands of people.
- On Twitter and LinkedIn, all posts, unless they are direct messages to another user, are visible to everyone (the whole world)
- If you are unsure of who can see your posts on other sites, you should always assume that the information is publicly available to all and could be found by people doing a search on Google, for example.

Before posting, staff and volunteers should ask themselves the following questions:

1. Do you want the whole world to see? Even if you restrict your own visibility settings, these can be overridden by the settings of others, or people can copy and paste the information into other, public, places.
2. Do you want the post to be seen forever? Once you have posted something, is it almost impossible to delete it again from the internet, even if you delete it from the site. There are sites that archive all Twitter posts, for example, so even if you delete a post from Twitter, it can still be found.

3. What if the information is taken out of context? It is very easy for others to take what is posted, alter it, and re-post it elsewhere. It is also possible that your hard work, posted online, may be used inappropriately by others.

4. Could the information put you or others in danger? What you post could tell others that your house is empty or that the pupils in your class are on a school trip, which could have implications for a looked-after child.
5. Are you violating any laws? The information could breach copyright, or specific legislation relating to privacy of vulnerable groups, for example. What you post could be illegal in other counties, which could have serious implications if you were to later visit there. Are you making claims that that could be taken as facts when they are not? This could lead you to being accused of slander
6. Is your message clear? Could you unintentionally be breaking cultural norms or putting out something unintentionally offensive. Is it clear whether or not you are posting in an official capacity?
7. Could the actions of your social networking friends reflect on you? Could your friends or friends or friends "tag" you in photographs or link you to inappropriate activities through their own posts? Choose your friends carefully.

If you have any doubts about any other these, you should seek the advice of the Head or DSL.

Access to inappropriate images

Although this is covered under the Acceptable Use Policy, there is an overlap with Social Networking, so these principles are re-stated here for the purpose of clarity:

- There are no circumstances that justify adults possessing indecent images of children. Staff or volunteers who access and/or possess links to such material or websites will be viewed as a significant and potential threat to children. This will lead to criminal investigation and disciplinary action. Where indecent images of children are found, the Head must be informed immediately.
- Adults must not use equipment belonging to the school to access any adult 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.
- Adults should ensure that pupils are not exposed to any inappropriate images or web links. The school endeavours to ensure that internet equipment used by pupils has the appropriate controls with regards to access. e.g. personal passwords should be kept confidential. Any potential issues identified must be reported to the Head immediately.
- Where other unsuitable material is found, which may not be illegal but which could or does raise concerns about a member of staff, high level advice should be sought before any investigation is conducted.
- Staff and volunteers should be aware that they could be drawn into an investigation of child pornography or obscene images if they are linked to someone under investigation through social networking sites. They should inform the Head immediately if they are contacted by the Police or other investigators.

Cyberbullying

Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

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

Adults are encouraged to report any, and all, incidents of cyberbullying to SLT/DSL or the Head.

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. Adults may wish to seek the support of their trade union or professional association representatives.

If the staff member or volunteer becomes aware of a pupil being subject to cyberbullying, they should raise it with the DSL, SLT or Head.