Ladygrove Primary School and Nursery

Social Media Policy

Reviewed September 2026

Due for next review September 2027

Writing and reviewing the Social Media policy:

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Online Safety Policy, Staff Code of Conduct, Acceptable Use Agreements, Data Protection Policy, Behaviour and Anti-Bullying Policy, Whistleblowing Policy, Complaints Policy, and Mobile Phone, Smartwatch and Photography policies. It reflects Keeping Children Safe in Education 2026, Working Together to Safeguard Children 2026, the Department for Education's current data protection guidance for schools, and its filtering and monitoring standards.

The policy is approved by the governing body and reviewed at least annually, and sooner where legislation, statutory guidance, technology, local procedures or school practice changes. The Headteacher and Designated Safeguarding Lead will ensure that staff, volunteers and governors understand the policy and receive appropriate updates.

All staff and workers at the school need to be aware of the risks and accountability of inappropriate or inadvertent provision of information about themselves, the school or 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 the Headteacher or a named representative may monitor such information.

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 in Telford)
- Anyone who could find your comments through search engines

Examples of Social Media and Social Networking sites and services include:

- Facebook
- X
- YouTube
- Instagram
- Snapchat
- LinkedIn
- Blogs
- Discussion groups
- Mailing Lists
- WhatsApp Messenger

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 Ladygrove Primary School and Nursery (or Telford & Wrekin Council).
- Activity carried out in the name of Ladygrove Primary School and Nursery, such as a school blog or Twitter posting or a Facebook group that represents, or appears to represent, the official views of the school.

This policy is not about stopping the use of – or accessing of – such groups but aims to ensure that the use of social media does not harm the interests of the children and young people we support or damages the reputation of the school or school staff.

Aim of this policy:

This policy recognises that social media is an integral and growing part of everyday life and makes 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 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 safe working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Prevent adults abusing or misusing their position of trust.

This document applies to all staff who work in the school whether paid or unpaid and includes members of the Governing Body.

Principles:

The principles that underpin this policy are:

- Adults who work with pupils 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 the document.

Why do we need the policy?

There have been numerous examples of people in all walks of life posting things in 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 because of your views, beliefs or comments

This has led to people facing disciplinary actions, 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.

Staff must remember that work-related content held on school or personal devices or accounts may be disclosable under data protection or information-access law. A subject access request (SAR) may cover relevant messages, images and other personal data. Staff must therefore use approved school systems for school business, communicate professionally, retain information in line with school procedures and never attempt to conceal or delete material connected with a concern, complaint, investigation or request. Advice must be sought promptly from the Headteacher, Designated Safeguarding Lead or Data Protection Officer.

Safer Social Networking Practice:

This document applies to current social networking sites such as Facebook, X, Instagram etc and all other current and emerging social media platforms.

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.

Safeguarding concerns and professional boundaries

Staff must use only school-approved accounts, platforms and devices to communicate with pupils about school matters. Personal accounts, private messaging, disappearing-message functions, livestreaming and one-to-one contact outside approved arrangements must not be used. Any online interaction, message, image or conduct that raises a safeguarding concern, including a low-level concern about an adult, must be recorded and reported without delay in accordance with the Child Protection and Safeguarding Policy. Staff must not investigate, forward or share such material beyond those who need to know; where possible, preserve the evidence and seek immediate advice from the Designated Safeguarding Lead. If there is immediate danger, emergency services must be contacted.

Artificial intelligence, deepfakes and manipulated content

AI-generated or digitally manipulated text, images, audio and video can create safeguarding, reputational, copyright and data protection risks. Staff must not use personal

data, confidential school information or identifiable images of pupils, families or colleagues in generative AI tools unless the tool and purpose have been formally approved and the processing complies with school policy. Staff must not create, share or endorse impersonations, deepfakes or misleading content. Suspected harmful, abusive or sexualised manipulated content must be treated as a safeguarding concern, preserved appropriately and reported immediately.

Filtering, monitoring and oversight

The school will maintain appropriate filtering and monitoring arrangements for school networks and devices, including consideration of real-time, dynamic, personalised and AI-generated content. A designated senior leader, supported by the Designated Safeguarding Lead and IT support, will review the provision at least once each academic year and following any significant safeguarding incident, system change or identified weakness. The governing body will receive appropriate assurance, and outcomes and actions will be recorded. Monitoring will be proportionate, lawful and transparent and will not replace staff vigilance, professional curiosity or prompt reporting.

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 of the Headteacher or Deputy Head before becoming 'friends' with ex-students once they reach adulthood
- Staff or volunteers should not be a 'friend' of a parent/carer of a pupil or ex-pupil of the school without seeking advice of the Headteacher or Deputy Head
- 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 Local Authority, their colleagues, or their 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 Local Authority. Doing so may results in disciplinary action being taken against them. If they have concerns about practices within the school or the actions of pupils or parents, they must act in accordance with the local authority's Whistle-Blowing Policy and the school's complaints procedure

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 photographs that may cause embarrassment to themselves and/or the school if they were to be published outside of the site.
- In their own interests, 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 associated families/friends having access to staff outside the school environment. It also reduces the potential for identity theft by third parties.

- 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 Headteacher where there may be implications for the adult and their position within the school setting.
- On leaving employment from the school, staff should review their social networking sites to ensure information relating to the school is accurate and appropriate.

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 (anyone can see them), visible to Friends (only people on their Friends list can see them) or visible to Friends of Friends, which means that posts are visible to all the friends of friends, which could be many hundreds or even thousands of people.
- On X 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 (please check your settings to disable this), 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, it is almost impossible to delete it again from the internet, even if you delete it from the site. There are sites that archive all X posts, for example, so even if you delete a post from X, 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.

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 of friends “tag” you in photographs or link you to inappropriate activities through their own posts?

If you have any doubts about any of these points, you should seek the advice of the Headteacher or Deputy.

School's Social Media sites:

Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of Ladygrove Primary School and Nursery.
Any social media sites linked to Ladygrove Primary School and Nursery must be clearly demarcated with the school logo or name to ensure transparency and confidence in the site. Only authorised social media sites linked to the school should offer links back to the main school website. A request must be made by other social media sites linked to the school to authorise the use of links referring back to the school's main website.

Information provided must be worthwhile and accurate; what is published on the site will reflect on the school's image, reputation and services.

Staff must stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.

Staff members must respect their audience and be sensitive in the tone of language used when discussing topics that others may find controversial or objectionable.

The Headteacher, and website administrators, must take overall responsibility to ensure that the website is kept up to date and relevant by class teachers.

We advise staff not to 'like' or comment on any Ladygrove Facebook posts as this will draw parents/carers attention to their personal profiles.

Moderation of content:

Official school social media accounts must use robust security and privacy controls, including strong unique passwords and multi-factor authentication where available, with access restricted to authorised staff. Personal data, pupil names, location information and identifiable images or recordings must only be published where there is a clear lawful basis, appropriate permission where required and compliance with the school's data protection, safeguarding and photography procedures. Content must not reveal sensitive information, routines or locations that could place a child at risk.

The content and postings on the school's Social Media must be moderated. Moderation is the responsibility of the Headteacher and website administrators who run the sites. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.

Content that is discriminatory, threatening, abusive, unlawful or likely to place a child or adult at risk must not be approved or republished. It must be preserved where safe to do so and reported immediately to the Headteacher and Designated Safeguarding Lead, who will decide whether referral to the police, children's social care, the local authority designated officer, the platform, or another appropriate agency is required. Staff must not investigate the matter themselves or circulate harmful material unnecessarily.

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, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. 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.

Employees are encouraged to report any and all incidents of cyberbullying to their line manager or the Headteacher/Deputy. 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. Employees 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 their Headteacher or Deputy.

Policy- Document Status		
Date of Policy Creation	September 2023	Named Responsibility: Kirsty Stewart
Date of review completion	September 2026	Named Responsibility: Kirsty Stewart
Inception of new Policy	September 2027 review due	Named Responsibility: Kirsty Stewart
Date of Policy Adoption by Governing Body		**October 2026**