Wallop Primary School
Social Media Policy - 2025

Produced By:	K Simons, Headteacher
Approved for School: Headteacher: Katie Simons Date: 25.11.25	 (Signature)
Approved by Governing Body: Chair/Deputy Chair: J Hannan Date: 25.11.25	 (Signature)

Aims

This policy aims to ensure all staff use social media and ICT responsibly, safely and in line with safeguarding and data protection requirements set out in *KCSIE 2025* and other relevant legislation. It covers both personal and professional use of all online platforms, including current and emerging social media, messaging, and content-sharing sites. The policy seeks to protect pupils, staff, and the school's reputation by promoting safe, respectful, and appropriate online behaviour. It supports clear boundaries between personal and professional life, helps manage legal and reputational risks, and ensures consistency across the school in how social media and ICT are used for communication, learning, and engagement.

Use and Responsibilities

Social media, online tools, and emerging technologies can enhance teaching, learning, communication, and professional development when used responsibly. This policy promotes the safe, ethical, and professional use of all digital platforms by staff, governors, contractors, and trainees. All users must protect pupils, colleagues, and the school's reputation by keeping personal and professional lives separate, maintaining confidentiality, and upholding safeguarding and data protection principles at all times.

Any misuse of social media or technology (by staff, pupils, parents, or others) must be reported immediately to the Headteacher or Designated Safeguarding Lead. Inappropriate use may lead to disciplinary or legal action. Staff should act with honesty, respect, and professionalism online, avoid content that could bring the school into disrepute, and never share or comment on confidential or personal information. Staff should avoid posting or re-posting content that is overly political. The school will also provide support and protection to any employee who experiences online harassment linked to their professional role.

In line with *Keeping Children Safe in Education (KCSIE) 2025*, staff must exercise caution and professional judgment when using Artificial Intelligence (AI) tools or systems in any capacity. The following expectations apply:

Safeguarding and confidentiality: AI must never be used to process, share, or generate content containing personal, confidential, or identifiable information about pupils, parents, or colleagues.

Professional use: Any use of AI for educational or administrative purposes must align with school policy, be transparent, and support professional decision-making or teaching.

Integrity and accuracy: Staff remain responsible for verifying the accuracy and appropriateness of any information, resources, or communications produced with the assistance of AI.

Reputation and conduct: The use of AI outside of school (including for personal or professional social media,

content creation, or tutoring) must not bring the school into disrepute or compromise safeguarding principles.

Disclosure: Any concerns, errors, or potential breaches arising from the use of AI must be reported to the Headteacher or Designated Safeguarding Lead without delay.

Personal Use of Social Media

If staff choose to use social media personally, they must use it responsibly and maintain clear boundaries between their personal and professional lives. To protect privacy and uphold safeguarding principles, staff should avoid identifying themselves as employees of the school on personal social media platforms and must never communicate online with current or former pupils. This includes declining or not sending 'friend' or 'follow' requests.

Information gained through employment, such as details about pupils, families, colleagues, or the school, must never be shared, discussed, or referenced on personal accounts. Photographs, videos, or images of pupils must not be posted online under any circumstances unless approved through official school procedures.

Personal social media accounts must not be used for school communication, and staff should use only school-approved channels (e.g. school email) for professional contact. Staff are advised to review their privacy settings regularly, keep passwords secure, and be cautious about sharing personal information. Profile photos and content should reflect professionalism and avoid bringing the school into disrepute.

Where school WhatsApp groups are used for operational communication (e.g. staffing updates, reminders, or quick questions), they must not include the names or identifying details of any pupils. WhatsApp is classed as social media, and the same safeguarding, confidentiality, and conduct expectations apply. The Headteacher will act as the group administrator and will remove staff when they leave the school.

Any misuse of social media, especially involving pupils, parents, or colleagues, must be reported immediately to the Headteacher or Designated Safeguarding Lead.

Monitoring

The school may monitor the use of its ICT systems, internet, and email in line with the Acceptable Use Policy. Staff should not expect personal privacy when using school devices or networks. Monitoring will only take place when necessary and will follow agreed school investigation procedures.

While the school respects employees' privacy, posts made on personal social media accounts are considered public if they can be viewed by others. If content on any public platform breaches, or is suspected of breaching, this policy or other related policies (such as safeguarding or conduct), the school may investigate and take appropriate action.

Where concerns arise about online activity from non-employees (such as parents, carers, or members of the wider community) the school will investigate and respond appropriately, including supporting further action if required.

Staff Who Are Also Parents or Carers

Where staff members are also parents or carers within the school community, they must exercise professional judgment at all times. Any communication with pupils or families connected to the school should follow safeguarding and child protection policies and maintain clear professional boundaries. Staff should only connect or communicate with others in the school community on social media in an appropriate manner that is able to withstand professional scrutiny. Any safeguarding concerns must be reported immediately to the Designated Safeguarding Lead.

Risks

The school recognises the potential risks associated with internet and social media use and seeks to manage these effectively to protect pupils, staff, and the school's reputation.

Key risks include:

- Access to or sharing of inappropriate material
- Breaches of confidentiality or data protection
- Damage to the school's or an individual's professional reputation
- Cyberbullying or online harassment
- Disclosure of personal or sensitive information
- Inappropriate behaviour, criticism, or complaints on public platforms
- Loss or theft of personal data or digital devices
- Social engineering or phishing attempts
- The spread of misinformation or disinformation that could cause harm, undermine trust, or compromise safeguarding
- Malware or virus infections from unsafe sites
- Staff identifying themselves as school employees and making inappropriate or disparaging comments about the school, pupils, parents, or colleagues

All staff must act to minimise these risks by following this policy, the Staff Code of Conduct, and the Acceptable Use Policy.

External Communication with Parents and Carers

The school uses a range of channels to maintain positive relationships with parents and carers, including letters, telephone calls, email, the school website, newsletters, meetings, and official social media accounts. All communication must reflect the school's vision and values, be professional in tone, and support constructive engagement with families.

Staff must not contact parents, carers, or pupils through personal social media, personal email, or private messaging. All communication must take place through official school systems including the admin email address and Arbor. The school's Facebook page and other official platforms are managed centrally and are not owned or operated by individual staff members. Only authorised staff may post or manage content on official school social media accounts. Posts must support the school's aims, safeguard pupils, and maintain professionalism at all times. Staff must never use personal accounts for school business or share personal contact details with parents, carers, or pupils. On school trips or activities, staff should use a school mobile phone rather than a personal device.

Personal devices must never be used to store or share images of pupils. The school will provide suitable hardware and software for professional use where required.

School Website and Use of Images

The school's website is managed by the admin team and SLT who ensure content is accurate, appropriate, and

compliant with safeguarding and data protection standards.

Permission for using images of pupils is obtained through the school's consent procedures, which include specific reference to online use. Staff and governor images will only be used publicly (online or in print) with their consent. All images are carefully checked to ensure pupils with restricted permissions are never shown.

Cyberbullying and Online Harassment

The school takes cyberbullying and online harassment extremely seriously. Staff must not use social media, messaging platforms, or any online service to insult, intimidate, or defame pupils, families, colleagues, or the school. Cyberbullying includes any use of technology, such as email, messaging, or social media, to cause harm, distress, or humiliation, whether inside or outside of school.

Staff must report any incidents of online bullying or harassment to the Headteacher or Designated Safeguarding Lead immediately. Victims should preserve evidence (such as screenshots or message logs) and avoid deleting messages. The school will investigate all reports promptly and take appropriate action under relevant policies, including disciplinary or safeguarding procedures.

If staff are victims of online abuse from members of the public, they will be supported by their line manager and, where appropriate, occupational health. Where a criminal offence may have occurred, the police will be informed. In these incidents, the headteacher will support the member of staff and encourage them to seek support from the school absence insurance and from their union.

The Senior Leadership Team (SLT) has a duty of care to ensure a safe working environment free from bullying or harassment. All allegations of online abuse or harassment will be investigated promptly and fairly, with support provided to those affected. Staff should retain any evidence to assist investigations.

If the incident involves illegal or indecent content, staff must not save or forward the material. It should be secured safely and reported to the police immediately for further instruction. Any incident involving the Headteacher must be reported directly to the Chair of Governors.

Compliance and Review

All staff and governors are expected to read, understand, and comply with this policy. Breaches of the Social Media and ICT Policy may result in disciplinary action in line with the Staff Code of Conduct and other relevant policies. Where a potential criminal offence is identified, the matter will be referred to the appropriate authorities.

This policy should be read alongside the following documents:

- Keeping Children Safe in Education (KCSIE) 2025
- Child Protection and Safeguarding Policy
- Acceptable Use Policy
- Data Protection Policy
- Staff Code of Conduct
- Behaviour and Anti-Bullying Policy

The Headteacher is responsible for ensuring the consistent implementation of this policy and for promoting safe, responsible use of technology across the school. The Designated Safeguarding Lead (and DDSLs) will monitor any incidents or concerns arising from online activity and ensure appropriate reporting and follow-up.

This policy will be reviewed every two years, or sooner if required, to reflect changes in legislation, technology, or statutory guidance.