Social Media & Online Communications Policy

Draft:	February 2026
Ratified:	March 2026
Review:	March 2027

Chair of Governors: 

Headteacher: 

Ethos of The Orchard School

At The Orchard School, **Everyone Matters, Everyone Cares**. Our ethos is rooted in the belief that every child has the potential to grow, thrive, and succeed when provided with the right environment, relationships, and support. **The Orchard Way** guides everything we do, ensuring that our approach is therapeutic, inclusive, and centred on understanding behaviour as communication. We are committed to nurturing the social, emotional, and mental health (SEMH) needs of our pupils, recognising their unique challenges while celebrating their individuality. Through strong relationships and a culture of care, we create a school where every pupil feels safe, valued, and empowered to reach their full potential.

Principles of Our Ethos:

1. Respect for the Individual: Every pupil deserves respect, dignity, and the opportunity to be heard.
2. Relationships at the Heart of Learning: Positive, trusting relationships form the foundation of our work.
3. Equity and Inclusion: We ensure all pupils have access to the support they need to succeed.
4. Therapeutic and Nurturing Approaches: We integrate trauma-informed strategies to promote resilience.
5. High Expectations with Compassion: Balancing aspirations with understanding and personalisation.
6. Collaboration with Stakeholders: Families, carers, and agencies work together to support pupils.
7. A Safe and Predictable Environment: Structure and boundaries foster trust and confidence.
8. Restorative Practices: Addressing conflicts through understanding, accountability, and growth.

1) Mission & Ethos

At The Orchard School, Everyone Matters, Everyone Cares. We believe every child can grow, thrive and succeed when provided with the right environment, relationships and support. The Orchard Way guides everything we do: a therapeutic, inclusive approach that recognises behaviour as communication and places each pupil's Social, Emotional and Mental Health (SEMH) needs at the centre. We aim to create a safe digital culture in which pupils feel valued and empowered online and offline.

2) Policy Statement

This policy sets out how staff, pupils, parents/carers and partners use social media and online communications responsibly, supporting learning and community engagement without compromising safeguarding, confidentiality, professional conduct or data protection. It implements current Department for Education (DfE) expectations for online safety, filtering and monitoring, Prevent Duty, searching and confiscation, and data protection.

3) Scope & Definitions

- Applies to: all staff (including contractors, governors, volunteers), all pupils, all parents/carers, and visitors posting about the school.
- Covers: all social platforms (e.g., Facebook, Instagram, TikTok, X/Twitter, LinkedIn), messaging (e.g., WhatsApp, Teams/Google Chat), forums, blogs, livestreams, and content-sharing platforms; any use on school devices or networks and personal devices where the school, its staff or pupils are involved.
- Online risks: we use the "4 Cs" (content, contact, conduct, commerce) and explicitly address misinformation and disinformation, conspiracy theories, AI-generated harms and deepfakes.

4) Legal & Policy Framework

This policy should be read in conjunction with:

- Keeping Children Safe in Education (KCSIE) 2025 (statutory).

- DfE Digital & Technology Standards – Filtering & Monitoring (core standard); annual review and clearly assigned responsibilities.
- UK Safer Internet Centre: Appropriate Filtering & Monitoring definitions (supporting).
- Data Protection – UK GDPR / Data Protection Act 2018; DfE data protection guidance for schools.
- Prevent Duty: safeguarding learners vulnerable to radicalisation (education guidance).
- Searching, Screening and Confiscation in schools (DfE).
- Teaching Online Safety in Schools (non-statutory, curriculum embedding).
- RSHE – revised statutory guidance (to be fully implemented by September 2026) including content on deepfakes, online misogyny and misinformation.

5) Principles

- Safeguarding first: online harms are safeguarding concerns and are responded to with the same rigour as offline harms.
- Proportionate filtering & monitoring: we protect pupils while avoiding over-blocking that impedes education; we review effectiveness at least annually.
- Data minimisation & confidentiality: we process and share data lawfully and securely; we do not publish personal data without a clear lawful basis.
- Education & empowerment: online safety is embedded across the curriculum (Computing, RSHE, PSHE) and pastoral systems.
- SEMH-informed practice: we recognise and plan for SEMH-linked online vulnerabilities (impulsivity, dysregulation, social naivety, exploitation risk).

6) Roles & Responsibilities

Governing Body/Proprietor:

- Ensure appropriate filtering and monitoring systems are in place and reviewed annually.
- Scrutinise DSL reports on online safety and assure policy implementation.

Headteacher:

- Ensures policy adoption, resourcing, staff training, and cross-school compliance.

Designated Safeguarding Lead (DSL):

- Leads digital safeguarding; oversees filtering/monitoring; reviews incidents and trends; coordinates responses and training; liaises with external agencies (police, LA, Prevent).
  IT/Network Lead:

- Implements technical controls aligned to DfE standards and UKSIC guidance; documents configurations and access controls; participates in annual review.

All Staff:

- Model professional conduct online; follow acceptable use, safeguarding and data protection procedures; report concerns promptly.

Pupils:

- Follow behaviour/acceptable use rules; seek help and report concerns (self/peers).

Parents/Carers:

- Engage respectfully; use complaints procedures rather than social media escalation; support pupils' safe online habits.

7) Acceptable Use

7.1 Staff

- Maintain a clear separation of personal/professional online presence; no private messaging with pupils on personal accounts or platforms.
- Do not "friend/follow" pupils on personal accounts; use school-approved channels only.
- Do not discuss confidential school matters or share personal data on social media.
- Complete regular online safety training, including updates on misinformation/disinformation, AI-generated content and deepfakes.

7.2 Pupils

- Use social media responsibly; bullying/harassment, sharing harmful content, sending or requesting indecent images, doxxing or hate speech are prohibited and will be sanctioned.
- Learn how to evaluate information, manage privacy, and seek help.

7.3 Parents/Carers

- Engage respectfully online; do not publish defamatory, abusive or identifying content about pupils/staff. Use school complaints routes for concerns.
- Support school guidance on images and consent, and on pupils' device use.

7.4 Official School Accounts

- Only authorised staff may publish; posts must protect confidentiality and uphold professional standards.

8) Mobile, Smart Technology & Messaging

Use of mobile phones and smart devices on site follows our Behaviour and Acceptable Use policies. Staff use school systems for communications with pupils/parents. Confiscation or searching of devices is governed by DfE Searching, Screening and Confiscation guidance; where indecent images or criminal content are suspected, staff follow DSL direction and legal guidance.

9) Filtering & Monitoring (DfE Core Standard)

We maintain appropriate filtering and monitoring on the school network and school-managed devices, reviewed at least annually, with clearly assigned responsibilities (Governors, DSL, IT). We balance protection with educational access and guard against over-blocking. UKSIC definitions inform provision and we complete Data Protection Impact Assessments where appropriate.

- Named senior lead and DSL oversight, governance reporting and annual review.
- Documented technical configuration, alerting/escalation pathways, and response logs.
- Risk assessments addressing AI-generated content, deepfakes, scams, harmful communities, radicalisation, and misinformation.

10) Safeguarding, Confidentiality & Data Protection

- Safeguarding: any online safety concern (e.g., exploitation, harmful sexual behaviour, self-harm content, radicalisation risk, hate content) is reported immediately to the DSL and handled under Child Protection procedures.

- Confidentiality: no confidential information about pupils/staff is shared on social media or external platforms.
- Images/Video: we only publish images or video with a lawful basis (typically consent) and in line with our Data Protection and Use of Images procedures; we never identify vulnerable pupils.
- Data minimisation: staff must use secure, approved systems; avoid personal accounts and unapproved storage; report data breaches promptly.

11) Curriculum, RSHE & SEMH

Online safety and digital wellbeing are taught through Computing, PSHE and RSHE. By September 2026 we will fully implement updated RSHE content (e.g., deepfakes, online misogyny/incel culture, image-based abuse, scams, AI chatbots, misinformation). Teaching emphasises critical thinking, respectful online conduct, consent, and help-seeking pathways (school and external). Staff are trained to recognise online triggers for dysregulation, impulsive/risky posting, and social vulnerability and to implement proportionate support plans.

12) Prevent Duty (Online Radicalisation)

We assess and mitigate online radicalisation risks (including platform-based grooming, extremist propaganda, and conspiracy ecosystems). Staff (including DSL/IT) know how to refer to Prevent/Channel and how to manage incidents involving extremist content discovered online.

13) Alternative Provision (AP)

Where pupils attend Alternative Provision (AP), we seek assurance that the AP has appropriate filtering/monitoring, online safety education, staff training and incident procedures. Responsibilities are clarified in commissioning documentation and reviewed regularly.

14) Reporting, Response & Escalation

- Anyone (staff, pupils, parents) can report concerns to the DSL or via published channels. The DSL triages, records and responds.
- We preserve evidence (e.g., screenshots/URLs), conduct proportionate investigation, and liaise with police where appropriate.
- We use searching and confiscation powers for devices in line with DfE guidance.

- We notify parents/carers where appropriate, considering pupil safety and confidentiality.

15) Responding to Misuse

15.1 Staff

Inappropriate social media use or breach of confidentiality/professional standards will be managed under staff conduct/disciplinary procedures and referred to external agencies where required.

15.2 Pupils

Misuse is sanctioned under the Behaviour Policy (including for incidents outside school that affect school life, e.g., cyberbullying or harmful posts), with restorative and SEMH-informed support.

15.3 Parents/External Parties

Defamatory/abusive posts about staff or pupils may lead to proportionate action (request to remove, blocking/reporting, legal/police referral if threats/harassment).

16) Staff Development

Induction and ongoing training include online safety, filtering/monitoring awareness, misinformation/disinformation, AI/deepfakes, Prevent Duty, data protection, and searching/confiscation procedures.

17) Communication with Parents & Community

We provide guidance on home online safety, privacy settings, screen-time balance, responding to online incidents, and how to raise concerns. We signpost to trusted resources (e.g., Educate Against Hate, UK Safer Internet Centre, UKCIS).

18) Monitoring, Assurance & Review

The DSL and IT lead report termly to Governors on incidents, trends, filtering/monitoring performance, and training. Annual review uses the DfE Filtering & Monitoring standard and UKSIC definitions to assure effectiveness. Updates are made when DfE guidance changes.

19) Linked Policies

Child Protection & Safeguarding; Behaviour; Anti-Bullying; Acceptable Use (Staff/Pupil); Staff Code of Conduct; Data Protection/Use of Images; RSHE; Searching, Screening & Confiscation; Prevent Duty; Alternative Provision Agreement.

20) Appendices (Summaries)

Appendix A: Social Media Guidelines for Staff (Quick Reference)

- Use only school-approved platforms for pupil/parent communication.
- Never share personal contact details with pupils; avoid personal social connections (follow/friend).
- Check privacy settings regularly on personal accounts; assume anything posted could be public.
- If you see concerning content about a pupil, screenshot/record the URL and report to the DSL immediately.
- Do not comment publicly on school matters; use internal channels.

Appendix B: Social Media Guidelines for Pupils (Quick Reference)

- Be kind, respectful and safe online; do not share or request indecent images.
- Think before you post: protect your privacy and digital footprint.
- If something worries you, tell a trusted adult or the DSL; save evidence if safe to do so.
- Report bullying, hate content, sextortion or grooming attempts immediately.

Appendix C: Social Media Guidelines for Parents/Carers

- Raise concerns via school complaints procedures, not on social media.
- Do not post identifiable images of pupils without consent.
- Support your child's privacy settings and discuss critical thinking about online content.
- Contact the school promptly if you become aware of an online safeguarding issue.

Appendix D: Reporting & Investigation Procedure (Summary Flow)

- Report concern to DSL (or Headteacher if concern relates to staff conduct).
- DSL triages: safeguard, preserve evidence, decide on internal actions and referrals (police/Prevent/Children's Services) as required.

- Record on safeguarding system; update risk assessments and support plans as needed.
- Feedback to reporter/parents as appropriate; monitor and review outcomes.

Appendix E: Examples of Acceptable/Unacceptable Use

- Acceptable: celebrating school achievements on official channels; using approved class platforms.
- Unacceptable: posting confidential pupil information; private messaging between staff and pupils; sharing harmful or indecent content; doxxing or hate speech.

Appendix F: Disciplinary Pathways for Policy Breaches (Overview)

- Staff: managed under Staff Code of Conduct/HR policies; may involve LADO/police as required.
- Pupils: sanctions per Behaviour Policy, with restorative and SEMH-informed support.
- Parents/External: may include requests to remove content, access restrictions, or legal action.

References (Key Guidance)

- Keeping Children Safe in Education (KCSIE) 2025 – DfE.
- DfE: Meeting digital and technology standards in schools and colleges – Filtering & Monitoring (core standard).
- UK Safer Internet Centre: Appropriate Filtering & Monitoring definitions (2024).
- DfE Data protection in schools (UK GDPR / Data Protection Act 2018).
- Prevent Duty: safeguarding learners vulnerable to radicalisation (DfE).
- DfE: Searching, screening and confiscation in schools.
- Teaching online safety in schools (DfE).
- RSHE statutory guidance (updated 2025; implement by Sept 2026).

This policy promotes a positive digital culture while safeguarding the privacy, welfare and reputation of all members of The Orchard School community.