



Social Networking Policy

Information for Parents: This policy is available on request.

1 Introduction

The Ursuline Preparatory School recognises that increasing numbers of adults and children use social networking sites and applications, including Snapchat, Instagram, TikTok, WhatsApp, X, YouTube, Facebook and generative AI/chatbot platforms. Used well, these technologies bring opportunities to communicate, learn and engage. Used carelessly, they carry real risks to children's safety and wellbeing and to the reputation of the School and its staff.

Most social networking platforms set a minimum age of 13 for account holders, with some exceptions (click [here](#) for age restrictions for social media accounts). Research consistently shows that a significant number of primary-age children hold active accounts on these platforms, and schools should not assume that use of social media is confined to secondary-age pupils.

This policy, and its associated guidance, exists to protect staff, pupils and parents/carers, and to set out how the School's leadership will respond to inappropriate use of social networking sites and applications.

2 Purpose

The purpose of this policy is to ensure:

- the school is not exposed to legal risks.
- the reputation of the school is not adversely affected.
- children are protected from the specific safeguarding risks that arise through social networking, including contact, content, conduct and commercial/contract risks (see section 5);
- anyone associated with the School can clearly distinguish where content on social networking applications is legitimately representative of the School; and
- staff, pupils and parents/carers know how to report a concern.

3 Scope

This policy applies to all School stakeholders, referred to collectively as 'School representatives', including employees, Trustees/Governors, parents and carers, those with parental responsibility, pupils, and volunteers. It applies to all use of social networking applications for any School-related purpose, whether or not the individual is contributing in an official capacity, and regardless of the platform used.

4 Legal and Regulatory Framework

This policy has been written with regard to the following statutory guidance and legislation, and should be read alongside it:

- Keeping Children Safe in Education (2026) — statutory guidance, in force from 1 September 2026, including its provisions on online safety, the 4Cs framework (content, contact, conduct, commerce/contract) and the specific risks associated with generative AI (see section 8).
- Mobile Phones in Schools (DfE) — statutory guidance in force from 1 September 2026, requiring schools to be mobile phone-free environments by default. This policy should be read alongside the School's separate Mobile Phones Policy.
- Working Together to Safeguard Children (statutory guidance).
- The Prevent Duty (Counter-Terrorism and Security Act 2015), in relation to online radicalisation.
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- The Online Safety Act 2023 and associated Ofcom codes of practice.
- The Equality Act 2010.
- The Education (Independent School Standards) Regulations 2014, and the ISI framework against which the School is inspected.

5 Related Policies

This policy should be read alongside:

- Child Protection & Safeguarding Policy
- Staff Code of Conduct / Staff Behaviour Policy
- Mobile Phones Policy
- Anti-Bullying Policy
- Behaviour Policy
- IT Acceptable Use Policy
- E-Safety Policy
- Data Protection Policy and Privacy Notices
- Whistleblowing Policy and Low-Level Concerns procedure

6 Roles and Responsibilities

6.1 Designated Safeguarding Lead (DSL)

The DSL, contactable on safeguarding@ursulineprepwarley.co.uk, is responsible for online safety as part of their wider safeguarding responsibilities, including receiving and acting on reports of concerning online contact or content involving pupils.

6.2 ICT Coordinator

The ICT Coordinator, contactable on ict@ursulineprepwarley.co.uk, has overall responsibility for the technical aspects of online safety within the school. This includes managing the school's technical infrastructure and safety systems, as well as receiving and acting upon any reports of concerning online contact or content involving pupils. They will work closely with the DSL and the Headteacher and Governing Body dealing with online concerns involving both pupils and staff.

6.3 Headteacher and Governing Body

The Headteacher has overall responsibility for this policy and its implementation. The Governing Body/Proprietor Body is responsible for approving the policy and holding leadership to account for its effectiveness.

6.4 All staff

All staff are expected to have read Part One of Keeping Children Safe in Education in full, and to understand and follow this policy.

7 Use of Social Networking application/sites during school time

7.1 Use of social networking applications for personal purposes during working hours is not permitted.

7.2 When using social networking applications for any School-related purpose, School representatives must not:

- publish content that may result in an action for defamation, discrimination, breach of copyright, breach of data protection, or any other claim for damages — including material of an illegal, sexual or offensive nature that may bring the School into disrepute;
- use social networking to promote personal financial interests, commercial ventures or personal campaigns;
- have a pupil or former pupil under the age of 18 as a 'friend' or share information with;
- post in an abusive or hateful manner;
- act in a way that breaches the School's Staff Code of Conduct or related policies;
- breach the School's policies on misconduct, equal opportunities, or bullying and harassment;
- discuss or advise on School matters, staff, pupils or parents;
- identify themselves as a School representative, other than on professional networking platforms such as LinkedIn, or reference any staff member, pupil, parent, or School activity/event without the prior written permission of the Headteacher.

7.3 Staff should be aware that where out-of-work online activity causes reputational harm to the School or raises a safeguarding concern, the School may take action under its disciplinary procedures, up to and including dismissal, in accordance with employment law and its own Staff Code of Conduct.

8 Online Safety Risks: the 4Cs

In line with KCSIE 2026, this policy recognises that online risk falls into four overlapping categories, each of which now explicitly includes risks from generative AI:

- Content — exposure to illegal, inappropriate or harmful material, including AI-generated or manipulated images (deepfakes) and nude or semi-nude imagery that is wholly or partly AI-generated.
- Contact — harmful interactions with other users, including adults seeking inappropriate contact with children, and harmful interactions with generative AI chatbots or companion-style applications that simulate human interaction.

- **Conduct** — a child's own online behaviour that increases risk to themselves or others, including making, sending or receiving explicit images (including those generated using AI).
- **Commerce/Contract** — commercial risks such as inappropriate advertising, scams, or data harvesting through apps and platforms.

Staff should treat a disclosure or discovery involving any of the above as a safeguarding concern and follow the procedure in section 11.

9 Guidance for Staff

9.1 No member of staff should interact with any current pupil on a social networking site.

9.2 No member of staff should interact with any former pupil who is under the age of 18 on a social networking site. This means staff must not request access to a pupil's social media area, and must not accept a pupil's request for access to their own.

9.3 Where a staff member has a family connection to a pupil that creates a legitimate reason for online contact, this should be declared to the Headteacher. Such contact should not, in any event, take place during the working day using School equipment.

9.4 Staff should:

- use appropriate language in any public-facing comments;
- review and adjust their own privacy settings appropriately;
- ensure content they post is not, or could not be construed as, defamatory;
- only post information, opinions or media about the School or its events with prior authorisation.

9.5 If a pupil attempts to contact a staff member, or attempts to gain access to a staff member's personal social media area, the staff member must not engage and must report it to the DSL without delay. Parents/carers of the pupil concerned will be informed.

9.6 Designated members of staff, authorised by the Headteacher, may access the School's official social media accounts (for example, X and Instagram) to post material on behalf of the School, in line with the School's separate guidance on managing official accounts, and with regard to data protection requirements set out in section 12.

9.7 Reporting a concern about a colleague

Any member of staff who becomes aware of another adult's inappropriate online contact with, or conduct towards, a pupil — including behaviour that may not yet meet the threshold of a safeguarding referral — must report this in line with the School's Low-Level Concerns procedure and, where the threshold is met, the Allegations Against Staff procedure in the Child Protection & Safeguarding Policy. Concerns should never be resolved informally between colleagues.

10 Guidance for Pupils

- No pupil under the age of 13 should hold an account on a social networking platform that requires a minimum age of 13.
- Pupils must not access social networking sites during the school day.
- Mobile phones and smart devices are subject to the School's Mobile Phones Policy, in line with DfE statutory guidance requiring schools to be phone-free environments by default from 1 September 2026. This policy should be read alongside that document, including the procedure for confiscation, secure storage and return.
- Pupils must not attempt to contact a member of staff, or seek access to a staff member's personal social media area. Any pupil who does so, or any member of staff who becomes aware of this, must inform the DSL. Parents/carers will be informed.
- Pupils are taught, through the curriculum and pastoral programme, how to recognise and respond to online risks, including contact from strangers, harmful or upsetting content, pressure to share images (including AI-manipulated images), and how to report a concern to a trusted adult.
- A pupil who is worried about anything that has happened online — to them or to someone else — can raise it with any member of staff, their form tutor, or the DSL directly. No pupil will be blamed for reporting a concern.

11 Guidance for Parents and Carers

- Posts should not include other members of the School community — for example, photographs or videos of other pupils taken at School events — without the consent of those pupils' parents/carers, in line with the School's Data Protection Policy.
- Allegations about staff or pupils must not be made via social networking or messaging platforms. Concerns should be raised directly with the School through the Complaints Policy or, where there is a safeguarding element, with the DSL.
- Complaints about School staff must not be aired via social media or messaging platforms; this includes statements that could be considered defamatory. Parents/carers should use the School's formal Complaints Procedure.

12 Data Protection

The School processes personal data, including images of pupils, in accordance with the UK GDPR, the Data Protection Act 2018, and its own Data Protection Policy and Privacy Notices. In relation to social networking, this means:

- Photographs or videos of pupils will only be posted on the School's official social media accounts where the School holds appropriate consent, in line with its Data Protection Policy and Privacy Notice; consent preferences are recorded and can be withdrawn by parents/carers at any time.
- Staff managing official School accounts must not include pupils' full names alongside identifiable images unless specific consent has been given, and should be alert to incidental personal data in the background of images or videos (for example, other pupils, home addresses, or car registration plates).
- Any suspected personal data breach relating to social media — for example, a pupil image posted without consent, or personal data shared inappropriately — must be reported immediately in line with the School's Data Breach Procedure.
- Staff and parents/carers should note that platforms may apply their own data processing terms (including, in some cases, use of uploaded content to train AI models); the School does not accept liability for third-party platforms' data practices, but will exercise care in what it chooses to share on them.

13 Monitoring, Filtering and Reporting a Concern

13.1 The School maintains filtering and monitoring systems on its own network and devices, to reduce the risk of pupils accessing harmful online content while on School systems. These systems do not extend to personal devices or home use, which is why the education set out in section 10 is essential.

13.2 Any concern about a pupil's welfare arising from social networking use — whether encountered on or off School premises — should be reported to the DSL immediately, using the procedure set out in the Child Protection & Safeguarding Policy. Concerns about a staff member's conduct should be reported in line with section 9.7.

13.3 Where a concern indicates possible criminal activity (for example, grooming, indecent images, or harassment), the DSL will consider referral to the police and/or children's social care without delay, in line with statutory guidance.