



Social Media Protocol 2026 – 2028

Grandpont is committed to safeguarding and promoting the welfare of children, young people and adults at all times, and expects adults and young people connected to the school to share this commitment. Social media and social networking sites play an important role in the lives of many people, both personally and professionally.

It is essential to recognise that using these sites brings an element of risk, but equally can be utilised in many positive ways. This document gives clarity on Grandpont's expectations around the use of social media.

Purpose

This protocol protects children, families and staff when social media is used in connection with the school. It should be read with the Child Protection, Staff Behaviour/Code of Conduct, Online Safety, Data Protection, Mobile Phone/Camera and Whistleblowing policies.

Core principles

Use only school-authorized accounts, devices and communication channels for school business.

Never photograph, record, store or share children using a personal phone, camera, wearable or other device with imaging or sharing capability.

Post a child's image, name, work or other personal information only where the school has a lawful basis, the required permission, and the content has been approved. Do not reveal location, routines, attendance, health, safeguarding or family information.

Do not upload children's images, work, personal information or confidential school material to generative-AI tools or other unapproved third-party services.

Maintain professional boundaries: do not accept or initiate personal social-media connections with current children or use private/direct messaging to communicate with them. Communicate with parents/carers only through approved school channels.

Last reviewed	September 2026
Next review	September 2027

Do not discuss children, families, colleagues, incidents or school business on personal accounts, even without names. Privacy settings, disappearing messages and closed groups do not make a post private.

Personal posts must not imply that they represent the school or undermine professional standards, safeguarding or public trust. Do not use the school name, logo or branding without authority.

School accounts

Only authorised staff may create, administer or post from a school account. Content must be accurate, respectful, accessible and appropriate for the intended audience.

Use strong, unique passwords and multi-factor authentication where available. Keep access details secure; review account access regularly and remove it immediately when a role changes or ends.

Moderate comments and messages. Remove or hide harmful or identifying content, record it where needed for safeguarding, and escalate concerns before blocking or responding.

Safeguarding and reporting

Online concerns may involve content, contact, conduct or commerce, including cyberbullying, grooming, exploitation, scams, harmful or AI-generated material, and non-consensual images.

Report any concern about a child immediately to the DSL or deputy and follow the Child Protection Policy. Do not investigate, promise confidentiality, forward harmful content or engage with the account. Preserve evidence safely where this can be done without viewing, copying or sharing illegal material.

Concerns about an adult's conduct—including photographing a child contrary to policy, inappropriate online contact or boundary breaches—must be reported under the allegations/low-level concerns procedure. Use the whistleblowing procedure if necessary.

Report an account compromise, accidental disclosure or suspected data breach immediately to the Headteacher and the school's data-protection lead.

Oversight

The school will brief staff at induction, provide regular online-safety updates, and review this protocol within its annual online-safety risk assessment. Breaches may lead to safeguarding action, removal of access, disciplinary action and/or referral to external agencies.

Last reviewed	September 2026
Next review	September 2027