

Online Safety Policy

*This policy is applicable to all Governors, Staff, Associates, Volunteers / All Pupils /
Parents/Guardian /Visitors*

Statement of Intention

We are committed to fostering an environment that promotes **our vision** 'To continue to be recognised as a leading Prep school, providing unforgettable learning experiences which inspire our pupils to **Believe** in themselves, to **Persevere** and **Succeed** in all they do'.

Our policies are designed to support the diverse needs of all our pupils, our staff, and our community. This policy and its procedures have been developed with due regard for our duties and obligations, for the safeguarding and wellbeing of all our pupils.

Principles of the policy

Bowdon Preparatory School recognises that online safety is an integral part of safeguarding and child protection and adopts a child-centred, whole-school approach to keeping children safe online. Safeguarding is everyone's responsibility, and all members of the school community have a role in recognising, reporting and responding promptly to online concerns, understanding that harm may occur both online and offline and that these experiences are often interconnected. The school will promote safe and responsible use of technology, provide appropriate education, filtering and monitoring, listen to the voice of the child, share information appropriately and work in partnership with parents/carers and relevant agencies to provide children with the right help, support and protection at the right time, in accordance with KCSIE 2026 and Working Together to Safeguard Children 2026

Objectives of the policy

The objective of this policy is to ensure that Bowdon Preparatory School provides a safe, secure and age-appropriate digital environment in which pupils can learn, communicate and use technology confidently and responsibly. The school aims to prevent, identify and respond effectively to online harm; ensure that staff understand their safeguarding responsibilities and act promptly on concerns; maintain effective filtering and monitoring arrangements; and equip pupils with the knowledge, skills and resilience to recognise and manage online risks, including those associated with social media, harmful content and emerging technologies such as generative AI. The school will work in partnership with parents/carers and relevant agencies, sharing information appropriately where necessary to ensure children receive the right help and protection at the right time, in line with KCSIE 2026, Working Together to Safeguard Children 2026 and current statutory guidance.

Contents

Introduction	3
Roles and Responsibilities	3
Responding to and Recording Online Safety Concerns	4
Prevention and Online Safety Learning	5
Emerging Technology and Artificial Intelligence (AI)	5
Images and Videos of Children	6
Filtering and Monitoring – SENSO	7
Related policies	7
Appendix A	8
Appendix B	9
Policy Review and Dissemination	11

Introduction

Digital technology is an integral part of teaching, learning, communication and the day-to-day operation of Bowdon Preparatory School. It provides pupils with valuable opportunities to learn, create, communicate and develop the digital skills they need for an increasingly connected world. Alongside these benefits, the rapidly changing online environment presents a range of safeguarding, wellbeing, privacy and security considerations that schools must understand and manage effectively.

This Online Safety Policy sets out the school's framework for the safe, responsible and appropriate use of digital technology and online services. It defines the roles and responsibilities of staff, pupils, governors, parents/carers and other members of the school community; establishes expectations for the use of school systems, networks, devices and personal technology; and outlines how online safety concerns and incidents will be identified, reported, recorded and managed. It also provides the framework for the school's approach to filtering and monitoring, social media, online communication, cyber security, data protection, mobile and smart devices, harmful online content and emerging technologies, including generative artificial intelligence (AI).

The policy applies to online activity that takes place within school and, where relevant to safeguarding or the welfare of pupils, outside the school environment. It recognises that technology, platforms and online risks continue to develop and therefore provides a framework that can respond appropriately to new and emerging issues.

Online safety is a shared responsibility across Bowdon Preparatory School. The Designated Safeguarding Lead (DSL) has overall responsibility for online safety and works closely with the Headteacher, Head of ICT, Network Manager and Curriculum Leads to ensure that safeguarding, technical security and online safety education are effectively coordinated. The DSL leads the safeguarding response to online concerns, reviews relevant filtering and monitoring information and ensures that concerns are recorded, assessed and escalated in accordance with the school's safeguarding procedures.

Roles and Responsibilities

The Headteacher provides strategic oversight and ensures that appropriate resources, policies, systems and staff training are in place. The Head of ICT and Network Manager have responsibility for the effective technical implementation and day-to-day management of the school's digital systems, including filtering, monitoring, network security and access controls. They work closely with the DSL to identify emerging risks, investigate technical concerns and provide appropriate reports and information to support safeguarding decisions. Technical staff do not make safeguarding decisions in isolation; where activity indicates a potential safeguarding concern, this is referred to the DSL.

Curriculum Leads ensure that appropriate opportunities for online safety education are embedded across the curriculum and reflect pupils' age, development and emerging risks. All staff are responsible for maintaining professional vigilance, modelling safe and responsible use of technology and reporting online safeguarding concerns promptly through the school's agreed procedures.

The school's leadership and governance arrangements provide appropriate oversight of online safety, including assurance that filtering and monitoring systems remain effective and are reviewed regularly.

Responding to and Recording Online Safety Concerns

Bowdon Preparatory School takes a coordinated, whole-school approach to identifying and responding to online safety concerns. Any online concern involving the safety or welfare of a pupil must be treated as a safeguarding concern and acted upon promptly. Staff must not investigate safeguarding concerns themselves but should report them in accordance with the school's safeguarding procedures and record the concern on CPOMS, providing a clear, factual and timely account.

The DSL should be informed without delay and will retain overall responsibility for assessing the safeguarding risk and determining the appropriate response. The DSL will work closely with the Headteacher, Head of ICT and Network Manager, as appropriate, particularly where technical information or action is required. Concerns may also be shared with relevant pastoral or curriculum staff where this is necessary to support the pupil.

Online concerns may be identified through a pupil disclosure, staff observation, information from parents/carers or another pupil, CPOMS, SENSO alerts, online activity or information received from an external agency. Concerns will be considered in the context of the individual child and any wider safeguarding information, recognising that online and offline harms are often interconnected.

Depending on the nature and level of risk, action may include pastoral or wellbeing support, communication with parents/carers where appropriate, additional online safety education, technical intervention, preservation of relevant information, or referral to external safeguarding agencies or the police. Where there is an immediate risk of serious harm or danger, 999 will be called.

All actions, decisions and outcomes relating to a safeguarding concern will be recorded appropriately on CPOMS. Information will be shared on a need-to-know basis and in accordance with the school's safeguarding and information-sharing procedures.

Prevention and Online Safety Learning

Prevention and education are central to the school's approach to online safety. Pupils are taught how to use technology safely, appropriately, responsibly and purposefully, both in and outside school, through ICT lessons, PSHE, assemblies and relevant areas of the wider curriculum. Online safety is treated as an ongoing and interrelated safeguarding theme rather than a one-off topic.

Teaching is age and developmentally appropriate and responds to current and emerging risks. It supports pupils to recognise unsafe or harmful situations, protect their privacy and personal information, understand appropriate online relationships and communication, evaluate the reliability of online information, develop critical thinking and know how, when and where to seek help.

Online safety education also supports pupils' mental health and wellbeing by helping them understand how online experiences, content and interactions can affect feelings, behaviour, relationships and self-esteem. Pupils are encouraged to develop healthy and balanced relationships with technology and to speak to a trusted adult when something online makes them feel worried, uncomfortable or unsafe.

The school's approach supports and promotes Fundamental British Values, including democracy, the rule of law, individual liberty, mutual respect and tolerance of those with different faiths and beliefs. Pupils are taught that these values also apply to their behaviour and interactions in the online environment.

Online safety messages are reinforced throughout the year, including through Safer Internet Day, Anti-Bullying Week, assemblies, pastoral activities and other appropriate whole-school initiatives. The school also works with parents/carers to promote consistent messages about safe and responsible technology use at home and at school.

Acceptable Use Agreements set out clear expectations for the use of technology and are shared with staff, pupils, parents/carers and other relevant members of the school community. Requirements relating specifically to social media are addressed within the school's separate Social Media Policy.

Emerging Technology and Artificial Intelligence (AI)

Bowdon Preparatory School recognises that artificial intelligence and emerging technologies provide significant educational opportunities but also introduce new safeguarding, privacy, ethical and educational risks. The school will take a proportionate, age-appropriate and safeguarding-led approach to their introduction and use.

Any AI or emerging technology used within school must be appropriate for its intended educational purpose and considered in relation to safeguarding, age suitability, privacy and data

protection, security, intellectual property, accuracy and bias. Staff and pupils must use approved systems in accordance with school policies and must not enter confidential, sensitive or personal information into AI systems unless the school has specifically approved that use and the necessary data-protection requirements have been satisfied. Current DfE guidance specifically identifies safeguarding, ethics, data and intellectual-property risks as areas schools must consider when using generative AI.

Pupils will be taught to understand that AI-generated material may be inaccurate, misleading, biased, manipulated or inappropriate and should not automatically be regarded as reliable. Teaching will develop critical thinking and appropriate use of AI while ensuring technology supports, rather than replaces, pupils' own learning, creativity and independent thinking.

Particular safeguarding consideration will be given to AI-generated or manipulated images, video, audio and text, including deepfakes and impersonation. Any use of AI that results in harmful, abusive, discriminatory, sexualised, threatening or otherwise inappropriate content involving a pupil will be treated seriously and, where appropriate, managed as a safeguarding concern.

The school will keep its approach under review as technology develops. When considering new AI products, the school will have regard to the DfE's Generative AI Product Safety Standards, which were expanded in January 2026 to address areas including cognitive development, emotional and social development, mental health and manipulation.

Images and Videos of Children

The school recognises that photographs and videos can support learning, celebrate achievement and provide a valuable record of school life. However, images and recordings of children constitute personal data where individuals can be identified and must be taken, stored, used and shared appropriately and securely.

The taking and use of photographs and video will be managed in accordance with the school's Data Protection, Privacy, Safeguarding and Acceptable Use arrangements, including any applicable parental permissions or other lawful basis. Staff must use school-approved devices, systems and platforms for school-related images and recordings and must follow school procedures regarding their storage, publication, sharing and deletion.

Particular care will be taken before publishing images or video online or through social media. The school will consider the purpose, audience, privacy and safeguarding implications of publication and will seek to minimise unnecessary identifying information.

Images and recordings of pupils must not be copied, altered, manipulated or uploaded to generative AI or other third-party services for unauthorised purposes. Any concern involving the creation, alteration, sharing or misuse of an image or video of a child, including AI-generated or manipulated content, must be reported immediately to the DSL and managed in accordance with the school's safeguarding procedures.

The DfE expanded its data-protection guidance in March 2026 specifically to provide additional guidance for schools on taking and using photographs and videos, alongside CCTV.

Filtering and Monitoring – SENSO

Bowdon Preparatory School uses SENSO filtering and monitoring software as part of its arrangements for protecting pupils when using the school's digital systems and network. Filtering and monitoring provide an important additional layer of safeguarding by helping the school identify inappropriate, harmful or concerning online activity and potential breaches of the school's Acceptable Use Agreements.

The DSL has safeguarding oversight of filtering and monitoring and works closely with the Head of ICT and Network Manager, who are responsible for the technical operation, maintenance and effectiveness of the system. Relevant SENSO alerts are reviewed and concerns are assessed according to their nature, context and level of risk. Where an alert or online activity raises a safeguarding concern, the DSL is notified and the concern is recorded on CPOMS and managed in accordance with the school's safeguarding procedures.

Weekly SENSO reports are reviewed to identify patterns, repeated incidents, emerging risks or changes in pupil behaviour. Information from these reports may be used to inform individual support, safeguarding intervention, curriculum planning, assemblies, staff awareness and wider online safety education.

Filtering and monitoring systems do not replace professional judgement or staff vigilance. Staff must report any online safeguarding concern even where it has not generated a SENSO alert. Equally, an alert should be considered in context and should not automatically be treated as evidence of wrongdoing.

The effectiveness of the school's filtering and monitoring arrangements will be formally reviewed at least annually and following any significant safeguarding incident, system change or identified emerging risk. Reviews will consider pupils' needs and risk profiles, the effectiveness of technical controls and developments in technology, including generative AI. This reflects the DfE's current Filtering and Monitoring Core Standard, updated in August 2026, which specifically incorporates consideration of generative AI risks.

Related policies

This policy should be read in conjunction with the following policies:

Safeguarding and Child Protection Policy

Acceptable use Agreement: Staff, Parents and Community

PSHE Policy

Data Protection Policy

Behaviour Policy

Anti-Bullying Policy

Social Media Policy

Appendix A

Relevant Legislation

This policy has been developed with regard to the following legislation, as amended and applicable to the school:

- **Children Act 1989** – provides the core legal framework for safeguarding children, including children in need and children suffering, or likely to suffer, significant harm.
- **Children Act 2004** – strengthens arrangements for safeguarding and promoting children's welfare and supports effective multi-agency working.
- **Education Act 1996** – forms part of the statutory framework governing education, pupil welfare and schools' responsibilities.
- **Education Act 2002** – establishes important duties relating to safeguarding and promoting the welfare of children in education.
- **Education and Inspections Act 2006** – provides schools with powers and responsibilities relating to pupil behaviour and discipline, including certain behaviour outside school.
- **Children's Wellbeing and Schools Act 2026** – strengthens the statutory framework relating to children's safeguarding, wellbeing and education.
- **Equality Act 2010** – protects individuals from discrimination, harassment and victimisation, including discriminatory or prejudicial behaviour occurring online.
- **Human Rights Act 1998** – protects fundamental rights, including privacy and freedom of expression, which must be balanced appropriately with safeguarding responsibilities.
- **Data Protection Act 2018** and UK GDPR – govern the collection, processing, storage, security and sharing of personal information and digital data.
- **Computer Misuse Act 1990** – creates offences relating to unauthorised access to, interference with and misuse of computer systems and data.
- **Copyright, Designs and Patents Act 1988** – governs copyright and intellectual property, including the lawful use, copying and sharing of digital material.
- **Protection from Harassment Act 1997** – provides protection against harassment, including repeated harmful behaviour conducted through electronic communications.
- **Protection of Children Act 1978** – contains offences relating to indecent photographs and pseudo-photographs of children, including relevant digitally created or altered imagery.
- **Sexual Offences Act 2003** – provides protection against sexual abuse and exploitation, including offences facilitated through online communication and digital technology.

- **Voyeurism (Offences) Act 2019** – introduced specific offences relating to certain forms of non-consensual intimate recording.
- **Domestic Abuse Act 2021** – provides the statutory framework relating to domestic abuse, including circumstances in which technology may facilitate controlling, coercive or abusive behaviour.
- **Counter-Terrorism and Security Act 2015** – establishes the statutory basis for the Prevent Duty, including the responsibility to consider risks of online radicalisation.
- **Online Safety Act 2023** – establishes the UK's regulatory framework for online services and includes duties designed to protect children from illegal and harmful online content and activity.
- **Malicious Communications Act 1988** – contains provisions relating to certain harmful or threatening communications.
- **Communications Act 2003** – forms part of the wider statutory framework governing electronic communications and certain communications offences.
- **Public Order Act 1986** – contains offences relating to threatening behaviour and stirring up hatred, including conduct that may occur online.
- **Education (Independent School Standards) Regulations 2014** (as amended) – establish the standards independent schools must meet, including requirements concerning safeguarding, pupil welfare, behaviour and education.

Appendix B

Statutory and National Guidance

This policy should be read alongside, and is informed by, the following current statutory and national guidance:

- **Keeping Children Safe in Education 2026 (KCSIE)** – statutory guidance for schools and colleges in England, effective from 1 September 2026. KCSIE establishes that online safety is an integral part of safeguarding and requires schools to protect children from online harm, ensure staff understand their safeguarding responsibilities, provide appropriate online-safety education and maintain effective filtering and monitoring arrangements. [Keeping Children Safe in Education 2026 – GOV.UK](#)
- **Working Together to Safeguard Children 2026** – statutory guidance setting out expectations for organisations and agencies working together to safeguard and promote the welfare of children. It recognises the significance of online harms, the interconnected nature of risks to children and the importance of timely information sharing, early help and effective multi-agency working. [Working Together to Safeguard Children – GOV.UK](#)
- **Prevent Duty Guidance: England and Wales** – statutory guidance supporting the duty under the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism. Schools must recognise and respond to

risks of radicalisation, including those arising through online content, platforms and activity. [Prevent Duty Guidance – GOV.UK](#)

- **Relationships Education, Relationships and Sex Education (RSE) and Health Education Statutory Guidance** – sets expectations for age-appropriate teaching about relationships, respectful behaviour, online safety and harms, digital resilience, privacy, consent and the safe and responsible use of technology. [Relationships Education, RSE and Health Education – GOV.UK](#)
- **Teaching Online Safety in Schools** – DfE guidance supporting schools in embedding online safety across the curriculum and teaching pupils to recognise, understand and manage online risks and make safe, informed decisions. [Teaching Online Safety in Schools – GOV.UK](#)
- **Filtering and Monitoring Core Standard** – DfE digital and technology standards setting expectations for effective filtering and monitoring arrangements. The school will ensure that responsibilities are clearly defined, systems are appropriate to the age and needs of pupils, safeguarding concerns are identified and acted upon, and provision is reviewed at least annually, taking account of changing technologies and emerging risks, including AI-generated content. [Filtering and Monitoring Core Standard – GOV.UK](#)
- **Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People** – UKCIS guidance informing the school's safeguarding response where children create, share or are affected by nude or semi-nude imagery, including digitally manipulated or AI-generated imagery where relevant. Incidents will be managed as safeguarding concerns rather than solely as behavioural matters. [Sharing Nudes and Semi-Nudes – GOV.UK](#)
- **Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers** – supports appropriate, proportionate and timely sharing of information where this is necessary to safeguard a child. Data protection legislation will not be treated as a barrier to sharing information where safeguarding requires it. [Safeguarding Practitioners Information Sharing Advice – GOV.UK](#)
- **Generative Artificial Intelligence (AI) in Education and DfE AI Safety Guidance** – informs the school's approach to the safe, responsible and appropriate use of generative AI, including safeguarding, data protection, age restrictions, intellectual property, misinformation and the potential creation or dissemination of harmful content. [Generative Artificial Intelligence in Education – GOV.UK](#)

Bowdon Preparatory School will have regard to revisions to statutory guidance and national standards and will review this policy at least annually, or sooner where changes in legislation, guidance, technology or emerging online safeguarding risks require it.

Policy Review and Dissemination

All members of staff and governors will receive a copy of this policy (via TEAMS link).

The policy will be available for parents on our website. A paper copy can be requested via the School Office office@bowdonprep.org.uk

SLT member responsible	S Hughes
Governor / Board Responsible	S Lees – Safeguarding Governor
Date of review	September 2026
Date of next review	September 2027