The Granville School ONLINE SAFETY POLICY – 2026/2027

(Including Early Years Foundation Stage)

Key Details

Designated Safeguarding Lead: Mrs Louise Lawrance Headmistress

Designated Safeguarding Deputy: Mrs Leah Harrington Deputy Headmistress

Designated Safeguarding Deputy: Mrs Jane Sladdin Head of Middle School

Named Governor for Safeguarding and Filtering & Monitoring: Mr Nick Arnold

Curriculum Leads: Miss Amanda Barrow Computing

Mrs Sarah Condren PHSE / RHSE

Network Manager: Mr Edward Cottingham

Date Updated: September 2026

Date agreed and ratified by Governing Body:

Date of next review: September 2027

This policy is a living document. It will be reviewed at least annually and amended during the year where necessary in response to safeguarding concerns, changes in technology, legislation, statutory guidance or the needs of the school community.

Updated September 2026
Next review September 2027

What is this policy?

Online safety is an essential part of safeguarding and child protection. Technology is now embedded within children's learning, friendships, entertainment and daily lives. The Granville School recognises both the opportunities and the risks this presents.

This policy reflects current statutory guidance including:

- Keeping Children Safe in Education (KCSIE)
- Teaching Online Safety in Schools (DfE)
- Education for a Connected World Framework (UKCIS)
- DfE Filtering and Monitoring Standards
- UK GDPR and Data Protection Act 2018
- The Online Safety Act 2023
- Children's Wellbeing and Schools Act 2026

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Acceptable Use Policies
- Data Protection Policy
- Cybersecurity Policy
- PSHE / RSHE Policy

Our Vision

At The Granville School, we believe online safety is not about fear. It is about helping children become thoughtful, kind, resilient and critical users of technology.

We aim to help pupils:

- stay safe online
- think critically
- understand the growing role of AI
- develop healthy digital habits
- communicate respectfully
- understand online influence and manipulation
- seek help confidently when worried

We recognise that technology will continue to evolve rapidly. Our goal is not simply to protect children from technology, but to help them become compassionate and responsible digital citizens who can navigate the online world wisely and confidently.

Our Whole School Approach

The Granville School adopts a proactive "little and often" approach to online safety education.

Rather than relying solely on assemblies or isolated lessons, pupils participate in:

- Computing curriculum online safety lessons
- PSHE / RSHE online safety education
- Weekly 10-minute Online Safety & Digital Literacy discussions at the start of Computing lessons from Reception to Year 6

These discussions follow a carefully sequenced whole-school progression model which revisits and develops key themes throughout the primary years including:

- online relationships
- privacy and security
- digital wellbeing
- misinformation
- respectful online behaviour
- AI literacy
- healthy screen habits
- critical thinking
- online reputation
- manipulation and persuasion online

This approach helps pupils gradually develop digital resilience, confidence and judgement over time.

Online Safety Curriculum

The school uses a cross-curricular approach based upon the UKCIS framework Education for a Connected World.

Online safety education is embedded across:

- Computing
- PSHE / RSHE
- Citizenship
- wider pastoral discussions
- assemblies
- safeguarding education

All staff are encouraged to identify opportunities to reinforce online safety themes across the curriculum and school life.

Supporting Pupils with SEND and Additional Needs

The school recognises that some pupils, including pupils with SEND, may be particularly vulnerable to online harms or may require additional support to recognise risk, understand boundaries or seek help.

Online safety teaching is adapted to meet individual needs. Where appropriate, the school will consider targeted interventions and additional technical safeguards, including specific filtering arrangements, to provide additional protection from online harm.

Weekly Online Safety & Digital Literacy Discussions

All pupils from Reception to Year 6 take part in weekly 10-minute Online Safety & Digital Literacy discussions during Computing lessons.

Sessions are designed to:

- encourage discussion
- develop awareness
- strengthen judgement
- normalise asking for help
- revisit safeguarding themes regularly

Themes include:

- kindness and respect
- passwords and privacy
- misinformation
- AI literacy
- scams and manipulation
- screen time balance
- healthy technology habits
- online wellbeing
- consent and boundaries
- reporting concerns

The programme progressively develops understanding from Reception through to Year 6.

Artificial Intelligence (AI)

The Granville School recognises that Artificial Intelligence is becoming an increasingly important part of children's digital lives. Our aim is not simply to restrict AI use, but to help pupils develop the critical thinking skills needed to question, evaluate and use AI safely, responsibly and ethically.

Pupils are taught:

- what AI is
- how AI systems learn
- that AI can make mistakes
- that AI-generated content may be inaccurate or biased
- that AI should not replace human thinking or creativity
- that AI tools may collect and store personal data
- that personal or sensitive information should never be shared with AI tools

The school also recognises emerging safeguarding concerns linked to:

- AI-generated misinformation
- deepfakes
- manipulated imagery
- AI chatbots
- emotional dependency on AI companions
- inappropriate AI-generated content

Staff and pupils are encouraged to approach AI with curiosity, caution and critical thinking.

Strategic Use of Generative AI

The school takes a risk-based and educationally purposeful approach to generative AI. Any generative AI platform used in school must be approved for its intended use, taking account of age restrictions, safeguarding, filtering and monitoring, data protection and the security of school information.

- Staff must use only school-authorised accounts and approved generative AI tools for school work.
- Personal, sensitive or confidential information about pupils, staff or the school must not be entered into generative AI tools.
- New AI-enabled platforms and services must be considered and approved before use, including appropriate data protection and safeguarding checks.
- Pupils may use generative AI in school only when it has been approved and is appropriate to their age, learning and the purpose of the lesson.
- AI-generated work must not be presented as a pupil's own independent work. Pupils are taught to acknowledge appropriate use and to check AI outputs critically.
- Staff, pupils and parents/carers are supported to understand both the creative possibilities and the safety, ethical and privacy implications of generative AI.

The school will keep its approach to generative AI under review as technology, national guidance and age-appropriate tools develop.

Current Online Safety Risks and Trends

The online world changes rapidly and safeguarding risks continue to evolve.

Current areas of concern nationally include:

- misinformation and fake news
- AI-generated content and deepfakes
- online bullying and group chat behaviour
- social media pressures
- online scams and phishing
- harmful influencers
- screen time and sleep disruption
- addictive app design and algorithms
- anonymous chat platforms
- inappropriate content
- grooming and exploitation
- image sharing risks

The school recognises that many children access online platforms below stated age restrictions. Our approach therefore focuses on realistic education, guidance and support rather than fear-based messaging alone.

Understanding Online Risk: the Four Cs

The school uses the established Four Cs model to help staff understand and recognise online safeguarding risks:

- Content – harmful or inappropriate material that pupils may see, hear or receive online, including misinformation and AI-generated content.
- Contact – harmful interaction with other people or systems online, including grooming, exploitation, scams and potentially unsafe interactions with generative AI or chatbots.
- Conduct – online behaviour that may cause harm, including bullying, coercion and the making, sending or receiving of explicit images, including images generated or manipulated using AI.
- Commerce – risks including inappropriate advertising, gambling, phishing, financial scams and other commercial pressures.

All staff are expected to recognise these areas of risk and report concerns to the DSL.

Online Safeguarding at The Granville School

The school regularly reviews the online experiences and emerging digital risks affecting its pupils. This is informed by pupil voice, safeguarding information, filtering and monitoring data, curriculum assessment and feedback from staff and parents/carers.

Findings are used to adapt the Computing and PSHE/RSHE curriculum, weekly Online Safety & Digital Literacy discussions, staff training and communication with parents/carers. This ensures that online safety education reflects the real experiences of pupils as well as national safeguarding priorities.

Digital Wellbeing

The Granville School recognises the growing impact technology can have on children's wellbeing, sleep, attention, emotional regulation and self-image.

Through Computing, PSHCE and weekly Online Safety discussions, pupils are encouraged to:

- develop healthy screen habits
- balance online and offline activities
- understand how apps and algorithms are designed to capture attention
- recognise the emotional impact of online interactions
- build healthy digital boundaries
- seek support when technology use negatively affects wellbeing

The school encourages healthy use of technology rather than excessive or passive screen use.

Critical Thinking and Misinformation

Pupils are taught that not all online information is trustworthy.

Children are encouraged to:

- question online content
- evaluate sources carefully
- recognise manipulation and persuasion
- identify scams and misleading content
- understand the influence of algorithms
- think critically before sharing information

This includes discussion of:

- influencers
- viral trends
- fake accounts
- clickbait
- AI-generated content
- online rumours
- conspiracy theories

Cybersecurity

The Granville School recognises that cybersecurity is an important part of safeguarding.

The school works with technical staff and external providers to:

- maintain secure systems and passwords
- protect school data
- reduce the risk of cyber attacks
- ensure backups and recovery systems are in place
- educate staff and pupils about phishing, scams and online security risks

Filtering and Monitoring

The school uses LGfL School Protect filtering systems and Lightspeed Alert monitoring systems to safeguard pupils online.

The DSL has lead responsibility for filtering and monitoring and works closely with the Network Manager, technical support and the named governor to ensure that the DfE Filtering and Monitoring Standards are implemented effectively.

The school follows the DfE Filtering and Monitoring Standards by:

- blocking harmful and inappropriate content
- monitoring safeguarding concerns
- reviewing systems regularly
- ensuring filtering supports teaching and learning appropriately

All staff are made aware of the school's filtering and monitoring systems and understand their responsibility to report:

- safeguarding concerns
- attempts to bypass filtering
- overblocking issues
- concerning online behaviour

Filtering and monitoring systems are reviewed:

- weekly by the DSL
- half-termly by technical staff
- annually as part of the online safety audit

All staff receive training regarding filtering and monitoring responsibilities.

Child-on-Child Abuse

The school adopts a zero-tolerance approach to all forms of child-on-child abuse including:

- online bullying
- sexual harassment
- image sharing abuse
- harmful online behaviour
- coercion or manipulation

All concerns are taken seriously and never dismissed as "banter" or part of growing up.

Sharing Nudes and Semi-Nudes

The school follows UKCIS guidance: *Sharing nudes and semi-nudes: advice for education settings*.

Staff understand that they must not:

- view
- copy
- print
- share
- delete

indecent images of children.

Any incidents or concerns will be referred immediately to the Designated Safeguarding Lead who will follow safeguarding procedures and seek external advice where appropriate.

Upskirting

Pupils are taught that upskirting is a serious invasion of privacy and a criminal offence.

Concerns relating to upskirting will be treated as safeguarding concerns and managed in line with KCSIE guidance.

Social Media

The Granville School expects all members of the school community to behave respectfully online.

Staff, pupils and parents should not:

- post abusive or harmful comments
- share confidential information
- engage in online bullying
- bring the school into disrepute

Parents and carers are encouraged to raise concerns directly with the school rather than through social media.

Members of the school community should avoid posting comments online which may harm individuals, staff wellbeing or the reputation of the school.

The school recognises that many pupils access social media below age restrictions and therefore provides age-appropriate education around:

- online friendships
- group chats
- online pressure
- healthy boundaries
- reporting concerns

Professional Conduct Online

Staff are expected to model safe, respectful and professional online behaviour at all times.

Staff must not:

- communicate with pupils through personal social media accounts
- share confidential school information online
- post content that could bring the school or profession into disrepute

Digital Images and Video

The school obtains parental permissions regarding the use of photographs and videos of pupils.

In light of the risk that generative AI can be used to manipulate photographs and create harmful, sexualised or misleading imagery, the school takes particular care when capturing, storing and publishing images of pupils and staff.

- Images of pupils or staff must not be altered, manipulated or used to create AI-generated content without explicit school authorisation and a legitimate educational or operational purpose.
- Any concern that an image of a pupil or member of staff has been manipulated, sexualised, shared without consent or used to create a deepfake must be reported immediately to the DSL.
- The school will keep its approach to publishing pupil and staff images under review in response to safeguarding guidance and developments in generative AI.

Staff must ensure that:

- images are appropriate

- pupils are treated respectfully
- personal data is protected
- images are stored securely

Pupils are taught:

- not to share images of others without permission
- to consider privacy and digital reputation
- to understand the risks associated with online image sharing

Use of Technology and Devices

School technology and online systems must always be used safely, responsibly and respectfully.

The school's Acceptable Use Policies outline expectations for:

- pupils
- staff
- governors
- volunteers
- contractors
- parents/carers

Pupils in Year 6 may bring mobile phones for emergency use only. Phones must remain switched off during the school day unless permission is given by staff.

Staff should keep personal mobile phones on silent during the school day and only use them in staff areas unless required for school purposes.

Visitors, volunteers and contractors should not use mobile phones in the presence of children unless authorised by the Headmistress.

Wearable Technology and Recording Devices

The same safeguarding expectations apply to wearable and recording-capable technology as to mobile phones. This includes smartwatches, smart glasses, cameras, audio recorders and other connected or wearable devices.

- Pupils must not use personal devices to photograph, video or audio-record pupils or staff during the school day unless expressly authorised for a school activity.
- Personal recording devices such as smart glasses are not permitted in school without written permission.
- Secret, covert or remote photography, video or audio recording of pupils or staff is prohibited.
- Visitors, volunteers and contractors must seek permission before using any recording-capable device on site.
- Where a wearable or connected device is required for an individual medical or accessibility need, appropriate arrangements will be agreed with the school.

Data Protection

The school follows UK GDPR and Data Protection Act 2018 requirements.

The school recognises that safeguarding and child protection take priority when necessary to protect children.

The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information where safeguarding concerns exist and where sharing information is necessary to protect children.

Reporting Concerns

Any online safety concern should be treated as a safeguarding concern.

All concerns must be reported immediately to the Designated Safeguarding Lead or Deputy DSL.

This includes concerns relating to:

- bullying
- grooming
- inappropriate content
- image sharing
- online exploitation
- harmful AI content
- wellbeing concerns
- extremist content
- scams or manipulation

The school follows safeguarding procedures outlined in the Child Protection and Safeguarding Policy.

The Granville School aims to create a culture where pupils feel safe discussing online experiences and know that concerns will be listened to calmly, seriously and without judgement.

Mandatory Reporting of Child Sexual Abuse

The school recognises the mandatory duty to report child sexual abuse introduced by the Children's Wellbeing and Schools Act 2026. Where information or an online safety incident indicates that a child may have been sexually abused, staff must report the concern immediately to the DSL and follow the school's safeguarding and child protection procedures.

The DSL will ensure that statutory reporting duties and referrals to the appropriate safeguarding agencies are carried out in accordance with current legislation and guidance. Staff must not investigate such concerns themselves or delay reporting while seeking further evidence.

Safer Internet Day

Safer Internet Day provides an opportunity to:

- revisit key safeguarding themes
- celebrate positive uses of technology
- encourage pupil voice
- reflect on digital wellbeing
- strengthen online safety awareness across the school community

Monitoring and Review

Online safety provision is reviewed annually through:

- safeguarding reviews
- curriculum evaluation
- pupil voice
- staff feedback
- governor oversight
- filtering and monitoring reviews

- the school online safety audit

The school will continue to adapt its provision in response to new technologies and emerging safeguarding concerns.

The Online Safety Policy and all Acceptable Use Policies are reviewed together to ensure that expectations remain consistent. The policy is communicated through staff induction and safeguarding updates, pupil education and age-appropriate AUPs, governor oversight and information for parents/carers.

Online safety themes and emerging concerns are shared with parents/carers through school communications, including regular newsletter updates linked to the weekly Online Safety & Digital Literacy discussions.

Roles and Responsibilities

Online safety is a shared responsibility across the whole school community.

All staff, governors, volunteers, parents and pupils are expected to:

- model respectful online behaviour
- report concerns promptly
- follow Acceptable Use Policies
- support a culture of safeguarding
- promote safe and responsible technology use

The Designated Safeguarding Lead maintains overall responsibility for online safety and filtering and monitoring systems.