Online Safety Policy

Prepared by: The Central Team

Date: September 2026

Version: V2.1

CONTENTS

Introduction
Aims
Legislation and guidance
Roles and responsibilities
Educating pupils about online safety
Educating parents/carers about online safety
Cyber-bullying
Acceptable use of the Internet in school
Pupils using mobile devices in school
Staff using work devices outside of school
How will the school respond to issues of misuse
Training
Links with other policies
Contact Information
Approval & Policy Review
Revision History
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)
Appendix 4: online safety training needs – self-audit for staff
Appendix 5: online safety incident report log

1. Introduction

Burlington House School, Tooting is owned and operated by Cavendish Education.

This Online Safety Policy forms part of the school's wider safeguarding arrangements and should be read alongside the Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Data Protection Policy, Acceptable Use Agreements, Cyber Security Policy, Mobile Phone Policy (where applicable), and other relevant safeguarding procedures.

The school recognises that technology plays an increasingly significant role in the lives of children and young people. Online safety is therefore viewed as an integral part of safeguarding and promoting the welfare of children, rather than a standalone ICT issue. Effective online safeguarding requires a whole-school approach involving leadership, governance, staff, pupils, parents and carers.

The school is committed to providing a safe learning environment in which pupils can benefit from technology whilst being protected from harm. We recognise that online risks continually evolve through developments in technology, including artificial intelligence (AI), social media platforms, gaming environments, live-streaming services, encrypted messaging applications and emerging online behaviours. Consequently, the school regularly reviews its online safety arrangements to ensure they remain effective and reflect current statutory guidance and emerging safeguarding risks.

This policy supports the school's commitment to:

- safeguarding and promoting the welfare of all pupils;
- developing pupils' knowledge, resilience and digital literacy;
- enabling staff to recognise and respond effectively to online safeguarding concerns;
- working in partnership with parents and carers to promote safe and responsible technology use;
- ensuring appropriate filtering, monitoring and cyber security arrangements are maintained across all school systems;
- promoting a culture in which safeguarding concerns arising online are identified, reported, managed and reviewed promptly.

The school recognises that online harms may occur both inside and outside school and that safeguarding incidents frequently involve both online and offline elements. Staff should therefore always consider whether concerns presented in one context may also have an online component.

This policy applies whenever pupils access technology provided by the school, use personal devices where permitted, participate in remote or blended learning, or where online activity may impact upon the safety or wellbeing of members of the school community.

The school acknowledges that online risks extend beyond traditional internet use and include, but are not limited to:

- exposure to harmful, illegal or inappropriate content;
- online grooming, exploitation and coercion;
- child-on-child abuse facilitated through technology;
- cyberbullying and online harassment;
- misinformation and disinformation;
- extremist and radicalising content;
- financial exploitation, fraud, phishing and sextortion;
- artificial intelligence, including deepfakes and AI-generated imagery;
- misuse of personal information and digital identities;
- technology-facilitated sexual violence and abuse.

The school is committed to ensuring that all online safeguarding arrangements are proportionate, risk-based and reviewed annually, or sooner where significant changes in technology, legislation or safeguarding guidance occur.

In the school's policies, unless the context requires otherwise, the word "parent" has the meaning given by Section 576 of the Education Act 1996 and includes any person with parental responsibility or who has care of the child, in accordance with current Department for Education guidance.

The school works with specialist external providers to support regulatory compliance and best practice, including services relating to:

- Human Resources and employment law;
- safeguarding and child protection;
- health and safety;
- Disclosure and Barring Service (DBS) checks;
- data protection and UK GDPR;
- cyber security and information security;
- online filtering and monitoring systems;
- mandatory staff training.

Where this policy refers to staff, this includes employees, agency workers, contractors, volunteers, governors and any other adults working on behalf of the school.

The school is committed to safeguarding and promoting the welfare of children and young people and expects every member of the school community to share this commitment. All decisions arising from this policy must place the safety, welfare and best interests of children at the centre of decision-making.

This policy is reviewed annually by the Governing Body and Senior Leadership Team, following advice from the Designated Safeguarding Lead (DSL), IT Lead and relevant safeguarding professionals. Additional reviews will be undertaken where changes to statutory guidance, technology or emerging safeguarding risks require earlier amendment.

2. Aims

The school recognises that technology provides significant educational, social and personal development opportunities for children and young people. Alongside these benefits, the school also recognises that digital technologies present safeguarding risks that require a proactive, whole-school approach to prevention, education and intervention.

This policy aims to:

- safeguard and promote the welfare of all pupils by ensuring they are protected from online harm both within and beyond the school environment;
- embed online safety as an integral part of the school's safeguarding culture, leadership, curriculum and daily practice;
- provide a safe digital environment that enables pupils, staff and the wider school community to use technology confidently, responsibly and securely;
- ensure robust systems are in place for identifying, reporting, recording, managing and reviewing online safety concerns;
- support pupils to develop the knowledge, skills, resilience and critical thinking needed to navigate an increasingly digital world safely;

- ensure staff understand their safeguarding responsibilities in relation to technology, emerging online risks and the appropriate use of digital tools, including generative artificial intelligence (AI);
- work collaboratively with parents and carers to promote consistent messages about safe and responsible technology use both at school and at home;
- maintain effective filtering, monitoring and cyber security arrangements that support safeguarding whilst enabling appropriate educational access;
- regularly review online safety arrangements in response to technological developments, emerging safeguarding risks and changes in statutory guidance.

2.1 The Four Categories of Online Risk

In accordance with statutory guidance, the school's approach to online safety is based on the four recognised categories of online risk:

2.1a Content
Being exposed to illegal, inappropriate or harmful material online, including but not limited to being exposed to illegal, inappropriate, or harmful content, for example:

- pornography,
- racism,
- misogyny,
- Self-harm,
- Suicide,
- Antisemitism,
- Radicalisation,
- Extremism,
- extreme sexual or physical violence,
- Misinformation,
- disinformation (including fake news) and conspiracy theories

2.1b Contact
Being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example:

- peer to peer pressure
- commercial advertising
- adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

2.1c Conduct
Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying

2.1d Commerce
Risks such as:

- online gambling,
- inappropriate advertising,
- phishing and or financial scams.
    - If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

2.2 Emerging Online Risks

The school recognises that online safeguarding risks evolve rapidly and will review this policy and associated risk assessments annually, or sooner where necessary.

Emerging risks currently include:

- generative artificial intelligence;
- deepfake images, audio and video;
- AI-generated sexual imagery;
- misinformation and disinformation;
- algorithm-driven harmful content;
- misogynistic influencers and online hate communities;
- encrypted messaging platforms;
- livestreaming platforms;
- online financial exploitation;
- technology-facilitated child-on-child abuse;
- online challenges and harmful trends;
- identity theft and impersonation.

The Designated Safeguarding Lead (DSL), Headteacher, IT Lead and Governing Body will ensure that the school's safeguarding arrangements continue to respond appropriately to these evolving risks through policy review, staff training, pupil education and effective filtering and monitoring arrangements.

3. Legislation and guidance

This policy has been developed in accordance with current legislation and statutory guidance relating to safeguarding, online safety, data protection and information security. It reflects the school's commitment to ensuring that online safety remains an integral component of safeguarding and child protection.

This policy should be read alongside the school's Child Protection and Safeguarding Policy and other related policies identified within Section 13.

The policy is informed by, but not limited to, the following legislation and guidance:

3.1 Department for Education Statutory Guidance

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children
- Information Sharing Duty: statutory guidance issued under section 16LA of the Children Act 2004 (September 2026). (including the statutory information sharing duty in section 16LA)
- Teaching Online Safety in Schools
- Relationships Education, Relationships and Sex Education (RSE) and Health Education
- Searching, Screening and Confiscation
- Behaviour in Schools
- Prevent Duty Guidance
- Meeting Digital and Technology Standards in Schools and Colleges
- Filtering and Monitoring Standards for Schools and Colleges

3.2 UK Council for Internet Safety (UKCIS)

The school follows relevant UKCIS guidance, including:

- Sharing nudes and semi-nudes: Advice for education settings working with children and young people
- Appropriate filtering and monitoring
- Digital resilience and online safeguarding resources
- Guidance relating to emerging technologies, including Artificial Intelligence, where applicable

3.3 National Cyber Security Centre (NCSC)

The school follows the principles published by the National Cyber Security Centre (NCSC), including guidance relating to:

- Cyber Essentials
- Multi-factor Authentication (MFA)
- Password management
- Phishing awareness
- Cyber incident reporting
- Secure cloud services
- Device security

3.4 Other Relevant Guidance

The school also has regard to guidance published by:

- CEOP Education
- Internet Matters
- Childnet
- NSPCC
- SWGfL
- Appropriate Local Safeguarding Partnership guidance where applicable.

3.5 Legislation

This policy reflects the requirements of relevant legislation, including, but not limited to:

- Education Act 1996
- Education Act 2002
- Education and Inspections Act 2006
- Education Act 2011
- Children Act 1989
- Children Act 2004
- Equality Act 2010
- Human Rights Act 1998
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Protection of Freedoms Act 2012
- Counter-Terrorism and Security Act 2015

Where staff suspect that online activity may constitute a safeguarding concern or criminal offence, the school will respond in accordance with statutory safeguarding guidance and, where appropriate, involve external agencies including Children's Social Care, the Police, Prevent partners or other relevant authorities.

3.6 Artificial Intelligence and Emerging Technologies

The school recognises that emerging technologies, including generative Artificial Intelligence (AI), continue to develop rapidly. While these technologies provide significant educational opportunities, they also present safeguarding, privacy, ethical and information security risks.

The school will ensure that:

- the use of AI is subject to appropriate safeguarding and risk assessment;
- staff receive appropriate guidance and training before adopting new AI technologies;
- pupils are taught to use AI safely, critically and responsibly;
- AI tools are used in accordance with data protection requirements and the school's Acceptable Use Agreements;
- this policy is reviewed whenever significant technological developments or changes in statutory guidance occur.

4.Roles and responsibilities

Safeguarding children online is everyone's responsibility. Effective online safety requires a coordinated, whole-school approach involving the Board of Directors, Local Governors, Senior Leadership Team, Designated Safeguarding Lead (DSL), IT staff, all employees, volunteers, pupils and parents/carers.
The school has clearly defined responsibilities to ensure appropriate governance, leadership, filtering and monitoring, cyber security, education and safeguarding arrangements are maintained.

4.1 The Board of Directors

The Board of Directors has strategic responsibility for ensuring that the school fulfils its safeguarding duties in relation to online safety.

The Board will:

- ensure that online safety is embedded within the school's safeguarding culture and strategic planning;
- ensure that this policy is reviewed and approved annually, or sooner where required;
- ensure appropriate filtering and monitoring systems are implemented, maintained and reviewed in accordance with the Department for Education's Filtering and Monitoring Standards;
- ensure sufficient resources are available to support effective safeguarding and cyber security arrangements;
- receive regular assurance reports regarding online safety, filtering, monitoring, cyber security and emerging risks;
- ensure annual online safety risk assessments are completed and appropriate actions implemented;
- ensure staff receive appropriate safeguarding and online safety training, including updates relating to artificial intelligence (AI), cyber security and emerging technologies;
- satisfy themselves that safeguarding responsibilities relating to online safety are being effectively discharged.

The Board will seek assurance that filtering and monitoring arrangements:

- are proportionate to safeguarding risks;
- are regularly tested and reviewed;
- do not unreasonably restrict teaching and learning;
- identify safeguarding concerns promptly;
- support effective safeguarding practice.

4.2 Local Governors

Local Governors are responsible for providing appropriate scrutiny and challenge regarding the school's online safety arrangements.

They will:

- understand their safeguarding responsibilities relating to online safety;
- receive regular reports on online safety, filtering and monitoring;
- review safeguarding trends and emerging online risks;
- monitor implementation of this policy;
- ensure safeguarding remains a standing agenda item during governance meetings where appropriate;
- support continuous improvement through challenge and oversight.

4.3 The Headteacher

The Headteacher has overall operational responsibility for ensuring that this policy is implemented consistently throughout the school.

The Headteacher will:

- promote a whole-school culture of online safeguarding;
- ensure online safety forms part of safeguarding practice across the curriculum;
- ensure appropriate staffing, resources and training are available;
- support the DSL in responding to safeguarding concerns;
- ensure staff understand their responsibilities under this policy;
- ensure safeguarding arrangements remain effective during remote and blended learning where applicable;
- oversee implementation of recommendations arising from online safety audits and risk assessments.

4.4 Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead has lead responsibility for online safeguarding.

The DSL will:

- oversee the implementation of this policy;
- ensure online safety is fully integrated within safeguarding procedures;
- work closely with the Headteacher, Governors, and the senior digital Lead to review online safeguarding arrangements;
- oversee the effectiveness of filtering and monitoring systems from a safeguarding perspective;
- ensure safeguarding concerns generated through monitoring systems are assessed promptly;
- manage all online safeguarding incidents in accordance with the Child Protection and Safeguarding Policy;
- maintain accurate records of online safeguarding concerns and analyse trends;
- coordinate safeguarding responses involving online abuse, exploitation or technology-facilitated harm;
- ensure appropriate referrals are made to Children's Social Care, the Police or other agencies where required; and ensure relevant information is shared with other relevant persons where the section 16LA of the Children Act 2004 criteria are met, including before a referral threshold is reached where sharing may facilitate safeguarding or welfare functions
- undertake and coordinate the annual Online Safety Risk Assessment;
- provide regular reports to Governors and Senior Leaders;

- coordinate staff safeguarding training relating to online safety and emerging technologies;
- monitor emerging online risks, including developments in artificial intelligence, deepfakes, online exploitation, misinformation and harmful online trends.

4.5 Senior Digital Lead

The school will identify an appropriately qualified member of staff with responsibility for the operational management of filtering, monitoring and cyber security systems. In some schools, this role may be undertaken by the IT Manager; in others, responsibilities may be shared. In BHST with some shared responsibility The DSL and IT manager share this responsibility.

The Senior Digital Lead will:

- maintain effective filtering and monitoring systems across school devices and networks;
- review filtering rules regularly to ensure they remain appropriate;
- work closely with the DSL regarding safeguarding alerts generated through monitoring systems;
- ensure monitoring systems support safeguarding without creating unnecessary barriers to teaching and learning;
- maintain secure network infrastructure;
- oversee cyber security arrangements;
- implement appropriate access controls and account management procedures;
- ensure software, operating systems and security updates are applied promptly;
- maintain secure backup arrangements;
- support cyber incident investigations;
- advise senior leaders regarding new technologies and associated risks.

4.6 All Staff, Volunteers, Contractors and Agency Staff

Every adult working on behalf of the school has a responsibility to safeguard children online.

All staff will:

- read and comply with this policy;
- understand that online safety is part of safeguarding;
- maintain appropriate professional boundaries online;
- follow the school's Acceptable Use Agreements;
- use school technology safely and responsibly;
- report concerns immediately using the school's safeguarding procedures; and provide relevant information promptly to the DSL so that statutory information-sharing duties can be discharged without delay
- understand how filtering and monitoring systems support safeguarding;
- report concerns regarding the effectiveness of filtering or monitoring systems;
- follow school procedures when authorised access to restricted content is required for educational purposes;
- remain alert to emerging online risks;
- complete required safeguarding and online safety training;
- understand the safeguarding implications of generative AI and other emerging technologies;
- never enter confidential or personally identifiable pupil information into unauthorised AI platforms or online services;
- promote safe and responsible technology use through everyday practice.

Staff should maintain an attitude of "it could happen here" when responding to online safeguarding concerns.

4.7 Pupils

Pupils are expected to:

- use technology responsibly and safely;
- follow the school's Acceptable Use Agreement;
- report anything online that causes concern;
- respect the privacy, dignity and wellbeing of others;
- avoid creating, sharing or requesting harmful or inappropriate content;
- use AI technologies only where authorised and in accordance with school expectations;
- contribute positively to a safe online environment.

4.8 Parents and Carers

Parents and carers play a vital role in supporting children's online safety.

The school encourages parents and carers to:

- reinforce safe online behaviours at home;
- engage with school guidance regarding online safety;
- supervise age-appropriate technology use;
- encourage children to report concerns;
- understand current online risks, including AI, social media, gaming, financial scams and online exploitation;
- work in partnership with the school where safeguarding concerns arise.

4.9 Visitors

Visitors using school technology or accessing school networks are expected to comply with this policy and any applicable Acceptable Use Agreement.

Where appropriate, visitors will receive information regarding safeguarding expectations before accessing school systems.

4.10 Monitoring and Review

The effectiveness of these roles and responsibilities will be reviewed annually through:

- the Online Safety Risk Assessment;
- safeguarding audits;
- filtering and monitoring reviews;
- cyber security reviews;
- incident analysis;
- governor scrutiny;
- policy review.

Where improvements are identified, action plans will be developed and monitored by the Senior Leadership Team and Governing Body.

5. Educating pupils about online safety

The school recognises that effective online safety education is fundamental to safeguarding children and young people. Online safety education is embedded throughout the curriculum and wider school life to enable pupils to become safe, responsible, respectful and resilient digital citizens.

Teaching is progressive, age-appropriate and responsive to emerging technologies and safeguarding risks. It is delivered through Computing, Relationships Education, Relationships and Sex Education (RSE), PSHE, assemblies, pastoral programmes and other curriculum areas where appropriate.

Online safety education is not delivered as a one-off event but forms part of a continuous programme that develops pupils' knowledge, skills and judgement throughout their education.

The curriculum reflects current statutory guidance and is regularly reviewed to ensure it addresses new and emerging online risks.

5.1 Curriculum Objectives

The school aims to ensure that pupils:

- understand the benefits and opportunities that technology provides;
- use digital technologies safely, responsibly and respectfully;
- understand that online safety is an important aspect of personal safety and safeguarding;
- know how to recognise, avoid and report online harm;
- develop critical thinking skills when accessing information online;
- understand that online behaviour has real-world consequences;
- recognise when online activity becomes unsafe, unlawful or exploitative;
- know where and how to seek support if they are worried about something they experience online.

5.2 Online Safety Themes

Online safety education will include, but is not limited to, teaching about:

5.2a Personal Safety Online

Pupils will learn how to:

- keep personal information secure;
- protect passwords and authentication methods;
- recognise phishing attempts and online scams;
- identify fake websites and fraudulent communications;
- manage digital identities responsibly;
- understand location sharing and privacy settings;
- recognise online grooming and exploitation.

5.2b Healthy Online Relationships

Pupils will be taught:

- respectful online communication;
- appropriate digital behaviour;
- consent in online interactions;
- recognising coercive or controlling behaviour;
- healthy use of social media;
- recognising unhealthy online relationships;
- the importance of reporting concerns.

5.2c Child-on-Child Online Abuse

Pupils will learn about:

- cyberbullying;
- abusive messaging;
- image-based abuse;
- online sexual harassment;
- sharing nude and semi-nude images;
- AI-generated indecent images and deepfakes;
- technology-facilitated abuse;
- misogyny and discriminatory online behaviour.

They will understand that such behaviour is unacceptable, may constitute a criminal offence and will always be taken seriously by the school.

5.2d Artificial Intelligence (AI)

Pupils will receive age-appropriate education about Artificial Intelligence, including:

- what generative AI is;
- its educational benefits;
- its limitations and inaccuracies;
- bias and misinformation;
- deepfake technology;
- AI-generated images and videos;
- responsible use of AI for learning;
- protecting personal information when using AI tools;
- recognising AI-generated scams and manipulation.

Pupils will understand that AI-generated content should not automatically be regarded as accurate or trustworthy and should be critically evaluated using reliable sources.

5.2e Misinformation and Disinformation

Pupils will be taught how to:

- evaluate online information critically;
- identify fake news;
- recognise manipulated media;
- identify unreliable sources;
- understand algorithms and personalised content;
- avoid sharing misleading information.

5.2f Online Financial Safety

Teaching will include awareness of:

- phishing;
- financial scams;
- identity theft;
- cryptocurrency scams;
- online gambling;
- in-app purchases;
- subscription traps;
- financial sextortion.

5.2g Digital Wellbeing

The curriculum will promote healthy technology use by helping pupils understand:

- balanced screen time;

- healthy online habits;
- digital wellbeing;
- the impact of excessive technology use on physical and mental health;
- strategies for maintaining positive online experiences.

5.3 Age-Appropriate Teaching

Online safety education will be carefully planned to reflect pupils':

- age;
- maturity;
- stage of development;
- individual needs;
- vulnerability;
- additional learning needs.

Teaching will be adapted where necessary for pupils with Special Educational Needs and Disabilities (SEND), pupils with communication needs, children in need, looked-after children, previously looked-after children and any pupils who may be particularly vulnerable online.

Staff recognise that a "one size fits all" approach may not be appropriate and will personalise learning where necessary.

5.4 Responding to Emerging Risks

Curriculum content will be reviewed regularly to ensure it reflects current safeguarding issues, including:

- emerging technologies;
- Artificial Intelligence;
- deepfakes;
- online influencers;
- misogynistic content;
- extremist narratives;
- harmful online challenges;
- evolving social media platforms;
- gaming environments;
- new forms of online exploitation.

5.5 Creating a Safe Reporting Culture

The school encourages pupils to report concerns about anything they experience online.

Pupils are regularly reminded:

- how to report concerns;
- who they can speak to;
- that they will be listened to;
- that safeguarding concerns will always be taken seriously;
- that seeking help is a positive and responsible action.

Where appropriate, pupils will also be signposted to external sources of support, including CEOP, Childline and other recognised safeguarding organisations.

5.6 Monitoring Curriculum Effectiveness

The school will regularly review the effectiveness of its online safety curriculum by considering:

- safeguarding trends;
- pupil voice;
- incidents recorded;
- staff feedback;
- curriculum reviews;
- local and national safeguarding intelligence;
- updates to statutory guidance.

Curriculum content will be amended whenever new safeguarding risks emerge.

6. Educating parents/carers about online safety

The school recognises that parents and carers play a vital role in helping children develop safe, responsible and positive online behaviours. Effective online safeguarding is most successful when schools and families work together to provide consistent messages and support.

The school is committed to maintaining open communication with parents and carers regarding online safety, emerging technologies and current safeguarding risks.

6.1 Partnership with Parents and Carers

The school will work collaboratively with parents and carers by:

- promoting a shared understanding of online safeguarding responsibilities;
- providing regular information and guidance about online safety;
- informing parents and carers of significant emerging online risks;
- encouraging safe and responsible technology use at home;
- supporting parents and carers to understand how the school's safeguarding arrangements protect children online;
- encouraging parents and carers to raise concerns promptly where they believe a child may be at risk online.

6.2 Information and Guidance

Parents and carers will receive online safety information through a range of appropriate methods, which may include:

- the school website;
- newsletters;
- parent information evenings;
- workshops or webinars;
- safeguarding updates;
- email communications;
- curriculum information;
- online safety campaigns such as Safer Internet Day.

Information shared with parents and carers may include guidance on:

- social media;
- online gaming;
- messaging platforms;

- smartphones and mobile devices;
- parental controls;
- age ratings;
- screen time and digital wellbeing;
- online relationships;
- cyberbullying;
- online financial scams;
- phishing and fraud;
- misinformation and fake news;
- Artificial Intelligence (AI);
- deepfakes and manipulated media;
- online grooming and exploitation;
- sextortion;
- reporting safeguarding concerns.

6.3 Artificial Intelligence (AI)

Recognising the increasing availability of generative Artificial Intelligence, the school will provide guidance to parents and carers to help them understand:

- how AI tools may be used appropriately for learning;
- the limitations of AI-generated information;
- safeguarding risks associated with AI;
- protecting personal information when using AI tools;
- recognising AI-generated scams, misinformation and deepfakes;
- how pupils are expected to use AI in accordance with the school's Acceptable Use Agreements.

6.4 Filtering and Monitoring

The school will explain, where appropriate, how it protects pupils through the use of filtering and monitoring systems.

Parents and carers will be informed that:

- filtering and monitoring systems operate on school devices and networks;
- these systems support safeguarding by identifying potential concerns;
- no filtering system can remove every online risk;
- pupils continue to require education, supervision and support to make safe choices online.

6.5 Supporting Safe Technology Use at Home

The school encourages parents and carers to:

- take an active interest in their child's online activity;
- discuss online experiences regularly;
- establish age-appropriate boundaries for technology use;
- supervise children's use of internet-enabled devices where appropriate;
- make use of parental controls and privacy settings;
- encourage respectful online behaviour;
- remind children that they can seek help whenever something online causes concern.

The school recognises that technology use outside school can directly affect pupils' safety and wellbeing within school and will work with families to address concerns wherever appropriate.

6.6 Reporting Concerns

Parents and carers are encouraged to contact the school if they have concerns regarding:

- cyberbullying;
- online abuse or exploitation;
- inappropriate online contact;
- concerning social media activity;
- misuse of Artificial Intelligence;
- online scams or financial exploitation affecting pupils;
- any online activity that may place a child at risk.

Concerns should normally be reported to the Designated Safeguarding Lead (DSL), Headteacher or another appropriate member of staff. Where section 16LA of the Children Act 2004 applies, relevant information must be shared proactively or in response to a request where it may facilitate another relevant person's safeguarding or welfare functions, subject to data protection requirements and the limited detriment exception.

Where concerns relate to an immediate safeguarding risk, the school will follow its Child Protection and Safeguarding procedures and involve external agencies where necessary.

6.7 Sources of Advice and Support

The school will signpost parents and carers to recognised organisations that provide reliable online safety advice and resources, including:

- UK Safer Internet Centre;
- Childnet;
- Internet Matters;
- NSPCC;
- CEOP Education;
- National Crime Agency CEOP Safety Centre;
- National Cyber Security Centre (NCSC).

Links to these organisations will be reviewed regularly to ensure that guidance remains current.

6.8 Review

The school's approach to parent engagement will be reviewed annually as part of the wider review of online safety arrangements. Feedback from parents and carers may be used to inform future communications, training opportunities and policy development.

7. Cyber-bullying

The school recognises that bullying and abuse increasingly occur through digital technologies and may have a significant impact on pupils' emotional wellbeing, mental health, safety and educational outcomes. Online abuse will be treated with the same seriousness as abuse occurring offline and will be managed in accordance with the school's Child Protection and Safeguarding Policy, Behaviour Policy and relevant statutory guidance.
The school recognises that safeguarding incidents frequently involve both online and offline elements. Staff will therefore consider whether concerns presented in one context indicate wider safeguarding risks.

7.1 Definition

Cyber-bullying is the use of digital technology to deliberately and repeatedly intimidate, threaten, harass, humiliate or harm another individual or group.

Cyber-bullying may take place through:

- social media platforms;
- messaging applications;
- online gaming;
- email;
- live-streaming services;
- online forums;
- websites;
- artificial intelligence (AI) platforms;
- image and video sharing services.

Online abuse may occur at any time and may continue beyond the school day.

7.2 Technology-Facilitated Child-on-Child Abuse

The school recognises that technology may be used to facilitate child-on-child abuse, including:

- cyber-bullying;
- online sexual harassment;
- abusive or threatening messages;
- image-based abuse;
- sharing or threatening to share intimate images;
- sharing nude or semi-nude images;
- AI-generated indecent images;
- deepfake images or videos;
- coercion and controlling behaviour;
- online hate incidents;
- misogynistic abuse;
- racist, homophobic, transphobic or other discriminatory abuse;
- online humiliation or exclusion;
- sextortion;
- online blackmail.

Such behaviour will always be treated as a safeguarding concern and managed proportionately in accordance with statutory guidance.

7.3 Preventing Online Abuse

The school seeks to prevent cyber-bullying and online abuse by:

- delivering a comprehensive online safety curriculum;
- promoting respectful online behaviour;
- educating pupils about consent and healthy online relationships;
- teaching pupils how to report concerns;
- maintaining appropriate filtering and monitoring systems;
- promoting positive digital citizenship;
- working collaboratively with parents and carers;
- responding promptly to emerging safeguarding risks.

All members of the school community are expected to contribute to creating a safe, respectful and inclusive online environment.

7.4 Reporting Concerns

Pupils are encouraged to report any online behaviour that causes them concern, whether they are:

- the victim;
- a witness;
- supporting another pupil.

Concerns may be reported to any trusted member of staff.

Staff receiving a report will:

- listen carefully;
- reassure the pupil;
- avoid making promises of confidentiality; and explain, in an age-appropriate way where safe and practicable, that relevant information may need to be shared to safeguard or promote welfare and that consent is not required where section 16LA of the Children Act 2004 applies
- record the concern promptly;
-
- inform the Designated Safeguarding Lead (DSL) in accordance with safeguarding procedures.

The school encourages a culture in which pupils feel confident that concerns will be taken seriously and acted upon appropriately.

7.5 Responding to Incidents

All incidents will be assessed on their individual circumstances.

Responses may include:

- safeguarding intervention;
- pastoral support;
- behaviour sanctions;
- restorative approaches where appropriate;
- parental involvement;
- risk assessments;
- referral to Children's Social Care;
- referral to the Police;
- involvement of external safeguarding agencies.

Where illegal content is identified, or there are reasonable grounds to believe a criminal offence has been committed, the school will preserve evidence where appropriate and consult the Police without unnecessary delay.

7.6 Sharing Nude and Semi-Nude Images

The school will manage incidents involving nude or semi-nude images in accordance with:

- the Department for Education's **Searching, Screening and Confiscation** guidance;
- UK Council for Internet Safety (UKCIS) guidance;
- Keeping Children Safe in Education;
- the Child Protection and Safeguarding Policy.

Staff will not request, copy, print, forward or share indecent images.

Where a member of staff believes a device contains an indecent image of a child or an AI-generated indecent image intended to depict a child, they will:

- not intentionally view the image unless absolutely necessary in accordance with statutory guidance;
- immediately confiscate the device where appropriate;
- report the matter to the DSL without delay;
- follow safeguarding procedures;
- preserve evidence where appropriate;
- seek Police advice where required.

7.7 Artificial Intelligence and Deepfake Abuse

The school recognises the increasing use of Artificial Intelligence to create realistic but false images, videos and audio recordings.

This may include:

- deepfake images;
- AI-generated intimate images;
- manipulated videos;
- impersonation;
- voice cloning;
- fabricated conversations.

Any use of AI to humiliate, threaten, exploit or abuse another individual will be treated as a serious safeguarding concern and may also constitute a criminal offence.

Incidents involving AI-generated abuse will be investigated in accordance with safeguarding procedures and may involve external agencies where appropriate.

7.8 Searching Electronic Devices

Authorised staff may search electronic devices where they have reasonable grounds to suspect that a device:

- contains evidence relating to a safeguarding concern;
- contains prohibited material;
- contains evidence of criminal activity;
- presents a risk to the safety or wellbeing of pupils or staff.

Searching will always be conducted lawfully, proportionately and in accordance with statutory guidance and the school's Behaviour Policy.

Where evidence may relate to a criminal offence, staff will not delete material and will preserve evidence for the Police.

7.9 Support for Pupils

The school recognises that pupils affected by online abuse may require ongoing support.
Support may include:

- pastoral support;
- safeguarding intervention;
- counselling where appropriate;

- mental health support;
- education regarding safe online behaviour;
- ongoing monitoring of wellbeing;
- support for parents and carers.

Support will be tailored to the needs of individual pupils.

7.10 Recording and Monitoring

All incidents of cyber-bullying and online abuse will be:
- recorded on the school's safeguarding recording system;
- monitored for patterns and trends;
- reviewed by the DSL;
- reported to senior leaders and governors where appropriate;
- used to inform future safeguarding education and policy review.

Lessons learned from incidents will contribute to the school's annual Online Safety Risk Assessment.

8. Acceptable use of the Internet in school

The school recognises that digital technologies play an important role in teaching, learning and the day-to-day operation of the school. All members of the school community are expected to use technology safely, responsibly, lawfully and in a manner that supports the safeguarding and wellbeing of others.

Acceptable use expectations apply whenever individuals are:
- using school-owned devices;
- accessing the school's network;
- using school accounts or cloud-based services;
- using personal devices where permitted;
- participating in remote or blended learning;
- undertaking school activities off-site where school technology is used.

All users must comply with the school's Acceptable Use Agreements (Appendices 1–3).

8.1 General Expectations

Users of the school's digital systems must:
- use technology primarily for educational or authorised professional purposes;
- behave respectfully towards others at all times;
- comply with safeguarding, behaviour and data protection requirements;
- protect personal and confidential information;
- report any online safety concerns immediately;
- follow the instructions of school staff regarding the safe use of technology;
- respect copyright, licensing and intellectual property rights.

Technology must never be used to:
- bully, intimidate or harass others;
- access, create, possess or distribute illegal, harmful or inappropriate material;
- deliberately bypass the school's filtering or monitoring systems without authorisation;
- impersonate another person;
- access another user's account without permission;

- disrupt school systems or network security;
- facilitate cheating or academic malpractice;
- engage in unlawful or discriminatory activity.

8.2 Filtering and Monitoring

To support safeguarding, the school operates appropriate filtering and monitoring systems across its devices and networks.

These systems are designed to:

- reduce the likelihood of pupils accessing harmful or inappropriate content;
- identify safeguarding concerns where appropriate;
- support staff in protecting pupils;
- assist the school in meeting its statutory safeguarding responsibilities.

Users should understand that:

- internet activity on school systems may be monitored;
- filtering systems cannot eliminate every online risk;
- monitoring is undertaken to protect the safety and wellbeing of members of the school community;
- concerns identified through monitoring may be investigated in accordance with safeguarding procedures.

Monitoring is carried out proportionately and in accordance with UK GDPR, the Data Protection Act 2018 and the school's Data Protection Policy.

8.3 Artificial Intelligence (AI)

The school recognises that generative Artificial Intelligence (AI) tools are increasingly available and may support learning when used appropriately.

The use of AI must always be:

- lawful;
- ethical;
- transparent;
- age-appropriate;
- consistent with safeguarding expectations;
- compliant with the school's AI and Acceptable Use guidance.

Users must not:

- enter confidential, personal or sensitive information into unauthorised AI platforms;
- use AI to generate abusive, discriminatory or harmful content;
- use AI to create or distribute deepfake images or manipulated media intended to cause harm;
- submit AI-generated work as their own where this breaches academic expectations;
- use AI in a manner that compromises safeguarding, privacy or information security.

Where AI is used for learning, pupils should acknowledge its use where required and remain responsible for checking the accuracy and reliability of any AI-generated content.

8.4 Personal Devices

The use of personal devices will be managed in accordance with the school's Mobile Phone Policy and

8.5 Acceptable Use Agreements.

Where personal devices are permitted, users must:

- use them responsibly;
- comply with safeguarding expectations;
- respect the privacy of others;
- avoid recording images, audio or video without appropriate permission;
- not use personal devices to circumvent school safeguarding arrangements.

8.6 Educational Platforms and Third-Party Applications

Only approved digital platforms and educational applications should be used for school activities.

Before introducing new digital services, the school will consider:

- safeguarding implications;
- data protection compliance;
- age appropriateness;
- cyber security;
- accessibility;
- educational value.

Staff must not require pupils to create accounts on unapproved platforms without authorisation.

8.7 Passwords and Account Security

Users are responsible for maintaining the security of their accounts.

They must:

- use strong passwords or passphrases;
- keep passwords confidential;
- use multi-factor authentication where available;
- lock devices when unattended;
- report suspected account compromise immediately;
- never share accounts or login credentials.

8.8 Social Media

Members of the school community should use social media responsibly and recognise that online behaviour may affect both personal and professional reputation.

Users should:

- maintain respectful online conduct;
- avoid posting content that could bring the school into disrepute;
- avoid communicating with pupils through personal social media accounts;
- comply with the Staff Code of Conduct and safeguarding expectations.

8.9 Remote and Blended Learning

Where technology is used to support remote or blended learning:

- only approved school platforms will be used;

- safeguarding expectations remain unchanged;
- professional boundaries must be maintained at all times;
- concerns arising during online learning must be reported immediately.

8.10 Responding to Misuse

Misuse of school technology will be addressed proportionately and may result in:

- withdrawal of access to technology;
- behaviour sanctions;
- safeguarding intervention;
- disciplinary action;
- referral to external agencies where appropriate;
- Police involvement where criminal activity is suspected.

The response will depend upon the nature, seriousness and circumstances of the incident.

8.11 Review

The school's Acceptable Use arrangements will be reviewed annually alongside this policy and updated where technological developments, safeguarding risks or statutory guidance require amendment.

9. Pupils using mobile devices in school

The school recognises that mobile phones and other internet-enabled devices can provide educational benefits but may also present significant safeguarding, wellbeing and behavioural risks. These include distraction from learning, cyberbullying, online abuse, unauthorised photography or recording, access to inappropriate content, and technology-facilitated child-on-child abuse.

In line with current Department for Education expectations, the school operates as a mobile phone-free environment during the school day, unless a specific educational, medical or safeguarding need has been authorised by the Headteacher or an appropriate member of the Senior Leadership Team.

9.1 General Expectations

Unless specifically authorised, pupils must:

- keep mobile phones switched off or on silent throughout the school day;
- store mobile phones securely in accordance with the school's procedures;
- not use mobile phones during lessons, breaktimes, lunchtimes, assemblies or other supervised school activities;
- not use mobile phones during educational visits unless authorised by staff;
- not use mobile phones in toilets, changing rooms or other areas where privacy is expected.

The school reserves the right to determine where and when mobile devices may be used.

9.2 Permitted Exceptions

The school recognises that there may be circumstances in which pupils require access to a mobile device.

Authorisation may be given where:

- a pupil has a documented medical need;

- a safeguarding or welfare plan requires access;
- the device is being used as part of a planned educational activity;
- a reasonable adjustment is required under the Equality Act 2010;
- exceptional circumstances have been approved by the Headteacher.

Any authorised use will be supervised and subject to appropriate safeguards.

9.3 Other Personal Devices

The expectations within this policy apply equally to:

- smart watches with communication functions;
- tablets;
- handheld gaming devices with internet access;
- wearable technology capable of recording images or audio;
- any internet-enabled personal device.

9.4 Safe and Responsible Use

Where pupils are authorised to use personal devices, they must:

- use devices responsibly and respectfully;
- comply with the school's Acceptable Use Agreement;
- respect the privacy and dignity of others;
- not photograph, film or record anyone without permission;
- not use devices to access inappropriate content;
- not attempt to bypass the school's filtering or safeguarding arrangements;
- immediately report any concerning online content or behaviour.

9.5 Artificial Intelligence and Mobile Devices

Pupils must not use mobile devices to:

- create or distribute AI-generated images intended to harm, embarrass or exploit another person;
- create or share deepfake images, videos or audio recordings;
- misuse generative AI during assessments or examinations;
- access unauthorised AI applications where prohibited by the school.

Any misuse of AI through personal devices will be treated as a safeguarding concern and managed in accordance with the school's Behaviour Policy and Child Protection and Safeguarding Policy.

9.6 Cyberbullying and Online Abuse

The school will investigate incidents involving personal devices where there is reason to believe that the use of a device has contributed to:

- cyberbullying;
- online harassment;
- sharing of indecent images;
- online sexual harassment;
- child-on-child abuse;
- sextortion;
- discriminatory behaviour;
- other safeguarding concerns.

This may apply regardless of whether the incident occurred during or outside the school day where it affects the safety or wellbeing of members of the school community.

9.7 Searching and Confiscation

Where authorised staff have reasonable grounds to believe that a mobile device contains evidence of misconduct, criminal activity or a safeguarding concern, they may search or confiscate the device in accordance with:

- the Department for Education's Searching, Screening and Confiscation guidance;
- Keeping Children Safe in Education
- the school's Behaviour Policy;
- the school's Child Protection and Safeguarding Policy.

Staff will act lawfully, proportionately and in the best interests of safeguarding.

Where evidence may relate to a criminal offence, the school will preserve evidence and consult the Police where appropriate.

9.8 Sanctions

Failure to comply with this policy may result in:

- confiscation of the device;
- behaviour sanctions;
- withdrawal of permission to bring a device into school;
- parental involvement;
- safeguarding intervention;
- disciplinary measures proportionate to the seriousness of the incident.

Serious incidents involving online abuse, indecent imagery, AI-generated abuse or criminal behaviour may be referred to external agencies.

9.9 Educational Visits

The use of mobile devices during educational visits will be determined following an appropriate risk assessment and communicated to pupils and parents before the visit.

Staff will consider:

- safeguarding;
- supervision;
- educational purpose;
- emergency communication;
- privacy;
- local circumstances.

9.10 Review

The school's arrangements relating to mobile devices will be reviewed annually as part of the Online Safety Risk Assessment and whenever changes to statutory guidance or safeguarding risks require amendment.

10. Staff using work devices outside of school

The school recognises that staff frequently use school-issued devices and digital systems away from the school site. The same standards of professional conduct, safeguarding, information security and acceptable use apply regardless of where school technology is used.

Staff are responsible for ensuring that school devices, systems and information remain secure and are used in a manner that protects pupils, colleagues and the wider school community.

10.1 General Expectations

Staff must:

- use school devices primarily for authorised school business;
- comply with the Staff Code of Conduct, Data Protection Policy, Acceptable Use Agreement and Cyber Security Policy;
- maintain appropriate professional boundaries when using technology;
- protect confidential and personal information at all times;
- immediately report any safeguarding, security or data protection concerns.

School devices must not be used for activities that are unlawful, inappropriate or likely to bring the school into disrepute.

10.2 Device Security

Staff are responsible for maintaining the security of any school-issued device.

This includes:

- using strong passwords or passphrases in accordance with school requirements;
- enabling multi-factor authentication (MFA) where available;
- ensuring devices automatically lock when unattended;
- never sharing login credentials;
- ensuring devices remain encrypted where required;
- keeping operating systems, applications and security software fully up to date;
- ensuring anti-virus and endpoint protection software remains active;
- securely storing devices when not in use;
- protecting devices from theft, loss or unauthorised access.

10.3 Secure Working Practices

When working away from school, staff must:

- use secure internet connections wherever possible;
- avoid accessing confidential information using unsecured public Wi-Fi unless protected by an approved VPN or equivalent security measures;
- lock screens whenever devices are left unattended;
- avoid discussing confidential information where conversations may be overheard;
- ensure confidential documents are not visible to unauthorised persons;
- securely dispose of printed confidential information.

10.4 Artificial Intelligence (AI)

Where Artificial Intelligence (AI) tools are used to support professional practice, staff must ensure that their use is consistent with safeguarding, professional standards and data protection legislation.

Staff must not:

- enter confidential pupil, parent or staff information into unauthorised AI systems;
- upload safeguarding records or sensitive documents to public AI platforms;
- rely solely on AI-generated information when making safeguarding, welfare or educational decisions;
- use AI to generate reports, references or professional documents without appropriate review and professional judgement;
- use AI to create misleading, discriminatory or inappropriate content.

Where AI is used to assist professional work, staff remain fully responsible for the accuracy, appropriateness and safeguarding implications of the final output.

10.5 Cloud Services and Digital Platforms

Staff must only use school-approved digital platforms and cloud services for storing or sharing school information.

School information must not be stored:

- on personal cloud storage accounts;
- on unauthorised external storage devices;
- within applications that have not been approved by the school.

Any new digital platform should undergo appropriate safeguarding, cyber security and data protection checks before use.

10.6 Use of Personal Devices

Where staff are authorised to access school systems using personal devices, they must ensure that:

- devices are password protected;
- software is kept up to date;
- security settings are enabled;
- confidential information is protected;
- school information is not shared with other users of the device.

Personal devices must not be used where doing so would compromise safeguarding or information security.

10.7 Cyber Security

Staff play an important role in protecting the school's cyber security.

Staff are expected to:

- recognise phishing emails and fraudulent communications;
- report suspected cyber incidents immediately;
- avoid opening suspicious attachments or links;
- protect authentication credentials;
- report lost or stolen devices without delay;
- comply with all school cyber security procedures.

10.8 Safeguarding Responsibilities

When working remotely, staff remain responsible for safeguarding pupils.

Staff must:

- maintain professional boundaries during online communication;
- use only approved school communication systems;
- report safeguarding concerns immediately using normal safeguarding procedures;
- ensure online meetings or remote learning sessions comply with school safeguarding expectations;
- remain alert to signs of online abuse, exploitation or other safeguarding concerns.

10.9 Lost, Stolen or Compromised Devices

If a school device is:

- lost;
- stolen;
- accessed by an unauthorised person; or
- suspected of being compromised,

staff must immediately notify:

- the Headteacher;
- the Designated Safeguarding Lead (where safeguarding information may be affected);
- the IT Lead or Filtering and Monitoring Lead.

The school will assess whether further action is required, including reporting a personal data breach where appropriate.

10.10 Monitoring and Compliance

The school reserves the right to monitor the use of school-owned devices and systems in accordance with:

- UK GDPR;
- the Data Protection Act 2018;
- the Investigatory Powers Act (where applicable);
- the school's Acceptable Use Agreement;
- safeguarding responsibilities.

Monitoring will always be proportionate, lawful and undertaken for legitimate educational, safeguarding, security or operational purposes.

Failure to comply with this policy may result in disciplinary action and, where appropriate, referral to external agencies.

11. How the school responds to issues of misuse

The school recognises that online safety incidents vary considerably in nature and severity. All concerns will be managed proportionately, consistently and in accordance with the school's safeguarding responsibilities, placing the welfare of the child at the centre of decision-making.

Where concerns indicate that a child may be at risk of harm, safeguarding procedures will always take precedence over disciplinary procedures.

The school will respond promptly to all concerns involving:

- cyberbullying;
- child-on-child online abuse;
- online grooming;
- online sexual harassment;
- sharing of nude or semi-nude images;
- AI-generated indecent images or deepfakes;
- online exploitation;
- extremist or terrorist content;
- online fraud or financial exploitation;
- misuse of Artificial Intelligence (AI);
- misuse of school technology;
- cyber security incidents;
- breaches of acceptable use agreements.

11.1 Reporting Online Safety Concerns

All members of the school community are expected to report online safety concerns as soon as they become aware of them.

Staff must:

- respond calmly and appropriately;
- listen to the child without judgement;
- reassure the pupil that they have done the right thing by reporting;
- avoid promising confidentiality;
- preserve evidence where appropriate;
- make an accurate written record;
- report the concern immediately to the Designated Safeguarding Lead (DSL).

Pupils should be encouraged to report concerns regardless of whether they are:

- directly affected;
- witnessing inappropriate behaviour;
- concerned about another pupil;
- uncertain whether behaviour is harmful.

11.2 Initial Assessment

The DSL (or deputy) will assess each incident to determine:

- whether the concern constitutes a safeguarding issue;
- whether immediate action is required to protect a child;
- whether criminal offences may have occurred;
- whether parents or carers should be informed;
- whether external agencies should be involved;
-
- what support is required for those affected.

The school will always adopt the principle of "it could happen here" when considering safeguarding concerns.

11.3 Safeguarding Response

Where a safeguarding concern is identified, the school will respond in accordance with the Child Protection and Safeguarding Policy.

Responses may include:

- immediate safeguarding intervention;
- risk assessment;
- increased pastoral support;
- referral to Children's Social Care;
- consultation with the Local Authority Designated Officer (LADO), where appropriate;
- referral to the Police;
- Prevent referral;
- referral to specialist support services.

The welfare of the child will remain the primary consideration throughout.

11.4 Behaviour and Disciplinary Responses

Where misuse of technology does not constitute a safeguarding concern but breaches school expectations, appropriate action may include:

- educational conversations;
- restorative approaches;
- withdrawal of technology access;
- confiscation of devices where permitted;
- behaviour sanctions;
- detention;
- suspension or exclusion in serious cases;
- staff disciplinary procedures where applicable.

Sanctions will always be proportionate to the nature and seriousness of the incident.

11.5 Artificial Intelligence (AI) Misuse

The school recognises that misuse of AI may present safeguarding, educational and legal concerns.

Examples include:

- creating deepfake images or videos;
- generating indecent or sexually explicit content;
- impersonating staff or pupils;
- using AI to facilitate bullying or harassment;
- generating misinformation;
- academic malpractice through unauthorised AI use;
- entering confidential school information into public AI systems.

Incidents involving AI will be assessed individually and managed through safeguarding procedures, behaviour procedures or disciplinary procedures as appropriate.

11.6 Cyber Security Incidents

Cyber security incidents may include:

- phishing attacks;
- malware infections;
- ransomware;
- unauthorised system access;

- compromised accounts;
- loss or theft of devices;
- suspected data breaches.

Staff must report cybersecurity concerns immediately to the IT Lead and Headteacher.

Where appropriate, the school will:
- isolate affected systems;
- preserve evidence;
- investigate the incident;
- notify relevant external agencies;
- consider data protection reporting requirements;
- review cyber security controls.

11.7 Evidence Preservation

Where incidents may involve criminal offences or safeguarding concerns, staff will:
- avoid deleting material;
- preserve electronic evidence where possible;
- avoid forwarding or copying indecent material;
- consult the DSL before taking further action;
- seek Police advice where appropriate.

The school will always follow current statutory guidance relating to searching, screening, confiscation and the management of indecent images.

11.8 Recording Online Safety Incidents

All online safety concerns will be recorded using the school's safeguarding recording procedures. Records should include decisions to share or not share relevant information under section 16LA of the Children Act 2004 and the rationale, including relevance, facilitation of safeguarding or welfare functions, and any detriment assessment and mitigation considered.

Records will include, where appropriate:
- the nature of the concern;
- date and time;
- individuals involved;
- actions taken;
- agencies involved;
- outcomes;
- follow-up support.

The DSL will monitor incidents to identify emerging patterns or recurring concerns.

11.9 Learning from Incidents

The school is committed to continuous improvement.

Following significant incidents, consideration will be given to whether improvements are required to:
- safeguarding procedures;
- staff training;

- curriculum provision;
- filtering and monitoring arrangements;
- cyber security controls;
- risk assessments;
- parental engagement;
- policy documentation.

Lessons learned will inform the school's annual Online Safety Risk Assessment and policy review.

11.10 Monitoring and Review

The Headteacher, DSL and Governing Body will receive regular information regarding online safety incidents to support effective safeguarding oversight.

Incident data will be reviewed periodically to identify:
- safeguarding trends;
- recurring online risks;
- emerging technologies;
- training needs;
- policy improvements.

Information shared with Governors will be anonymised where appropriate.

12. Training

The school recognises that effective online safety depends upon all members of the school community understanding their safeguarding responsibilities and maintaining up-to-date knowledge of emerging technologies, online risks and statutory guidance.

Online safety training forms an integral part of the school's safeguarding training programme and is delivered as part of induction, annual safeguarding updates and ongoing professional development.

Training is regularly reviewed to ensure it reflects current legislation, safeguarding practice and emerging online risks.

12.1 Staff Training

All staff, including agency staff, volunteers and contractors, will receive appropriate online safety training as part of their induction before working with pupils.

Training will include:
- the school's Online Safety Policy;
- safeguarding responsibilities relating to online safety;
- the staff Acceptable Use Agreement;
- recognising online abuse and exploitation;
- child-on-child online abuse;
- cyberbullying and online harassment;
- online grooming;
- sexual violence and sexual harassment online;
- sharing nude and semi-nude images;

- filtering and monitoring arrangements;
- reporting safeguarding concerns;
- professional use of technology;
- information security and cyber security;
- data protection responsibilities;
- Artificial Intelligence (AI), including opportunities and safeguarding risks;
- emerging online risks.

Staff will understand that safeguarding incidents often involve both online and offline elements and that online safety is everyone's responsibility.

12.2 Annual Refresher Training

All staff will receive online safety updates at least annually as part of safeguarding training.

Additional updates will be provided whenever there are significant changes to:
- statutory guidance;
- safeguarding risks;
- school procedures;
- filtering and monitoring arrangements;
- Artificial Intelligence technologies;
- cyber security threats.

Updates may be delivered through:
- staff meetings;
- safeguarding briefings;
- online learning modules;
- newsletters;
- email updates;
- external training events.

12.3 Artificial Intelligence (AI)

Recognising the rapid development of AI technologies, staff training will include:
- understanding generative AI;
- educational opportunities presented by AI;
- safeguarding risks associated with AI;
- deepfakes and manipulated media;
- AI-generated indecent imagery;
- misinformation and hallucinations;
- protecting personal and confidential information;
- ethical use of AI;
- academic integrity;
- recognising AI misuse by pupils.

Staff will understand that AI should support, rather than replace, professional judgement.

12.4 Cyber Security Training

Staff will receive appropriate cyber security awareness training, including:
- phishing awareness;

- password management;
- multi-factor authentication (MFA);
- secure remote working;
- recognising cyber attacks;
- secure use of cloud services;
- reporting cyber incidents;
- protecting school devices;
- secure handling of personal information.

Cyber security awareness will be refreshed regularly to reflect emerging threats.

12.5 Designated Safeguarding Lead (DSL)

The DSL and Deputy DSLs will undertake safeguarding training in accordance with statutory requirements.

This will include:
- advanced online safeguarding;
- emerging technologies;
- filtering and monitoring;
- Artificial Intelligence;
- technology-facilitated abuse;
- online exploitation;
- child-on-child online abuse;
- cyber security considerations relevant to safeguarding.

The DSL will maintain knowledge through:
- safeguarding networks;
- local authority updates;
- professional development;
- national guidance;
- specialist training.

12.6 Governors

The Local Governors will receive appropriate training to enable them to fulfil their strategic safeguarding responsibilities.

Training will include:
- statutory safeguarding responsibilities;
- online safety governance;
- filtering and monitoring standards;
- cyber security;
- Artificial Intelligence;
- emerging safeguarding risks;
- annual policy review;
- interpreting safeguarding assurance reports.

Governors should be able to provide effective challenge and oversight of the school's online safety arrangements.

12.7 IT Staff

Staff responsible for IT, filtering and monitoring systems will receive training appropriate to their roles, including:

- cyber security;
- filtering technologies;
- monitoring systems;
- safeguarding alerts;
- information security;
- incident response;
- data protection;
- secure infrastructure management.

12.8 Volunteers and Contractors

Volunteers, visiting professionals and contractors will receive online safety information proportionate to their role and level of contact with pupils.

Where appropriate, this will include:

- safeguarding expectations;
- acceptable use requirements;
- reporting procedures;
- confidentiality;
- professional conduct.

12.9 Pupil Education

Online safety education for pupils forms part of the school's wider curriculum and is delivered progressively throughout each key stage.

Teaching will include:

- safe online behaviour;
- cyberbullying;
- online relationships;
- privacy;
- password security;
- phishing and scams;
- misinformation;
- Artificial Intelligence;
- digital wellbeing;
- financial exploitation;
- online grooming;
- reporting concerns.

Teaching will be adapted to meet the needs of pupils with SEND and other vulnerable groups where appropriate.

12.10 Monitoring Training Effectiveness

The effectiveness of online safety training will be reviewed through:

- safeguarding audits;
- staff self-assessment;
- incident analysis;

- training evaluations;
- governor scrutiny;
- annual Online Safety Risk Assessment.

Where training needs are identified, additional learning opportunities will be provided.

12.11 Record Keeping

The school will maintain records of online safety training undertaken by staff, governors and, where appropriate, volunteers.

Training records will inform future professional development planning and support compliance with statutory safeguarding expectations.

13. Links with other policies

This Online Safety Policy forms part of the school's wider safeguarding framework and should be read alongside the following policies, procedures and guidance. Together, these documents support the school's commitment to safeguarding and promoting the welfare of children and ensuring the safe, secure and responsible use of technology.

13.1 Safeguarding Policies

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy
- Anti-Bullying Policy
- Relationships, Sex and Health Education (RSHE) Policy
- Attendance Policy (where relevant)
- Whistleblowing Policy
- Low-Level Concerns Policy
- Safeguarding Response to Children Missing Education (where applicable)

13.2 Technology and Information Governance

- Acceptable Use Agreements (Pupils, Staff, Governors, Volunteers and Visitors)
- Data Protection Policy
- UK GDPR Privacy Notices
- Cyber Security Policy
- Information Security Policy
- Bring Your Own Device (BYOD) Policy (where applicable)
- Mobile Phone Policy
- Artificial Intelligence (AI) Acceptable Use Policy (where applicable)
- ICT Network and Infrastructure Policy
- Records Management and Information Governance Policy

13.3 Teaching and Learning

- Computing Curriculum

- RSHE Curriculum
- PSHE Programme
- Remote Learning Policy
- Educational Visits Policy (where technology is used)
- Assessment Policy (including expectations for the use of AI)

13.4 Staff Employment Policies

- Disciplinary Policy
- Capability Policy
- Professional Conduct Expectations
- Flexible and Remote Working Policy (where applicable)

13.5 Health, Safety and Wellbeing

- Health and Safety Policy
- Mental Health and Wellbeing Policy
- Equality, Diversity and Inclusion Policy

13.6 National Guidance

This policy has been developed having regard to current statutory guidance and recognised good practice, including:

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children
- Teaching Online Safety in Schools
- Relationships Education, Relationships and Sex Education (RSE) and Health Education
- Searching, Screening and Confiscation
- DfE Filtering and Monitoring Standards
- DfE Meeting Digital and Technology Standards for Schools and Colleges
- UK Council for Internet Safety (UKCIS) Guidance
- National Cyber Security Centre (NCSC) Guidance
- CEOP Education Resources

14. Contact Information

Questions regarding this policy or concerns relating to online safety should be directed to:

Designated Safeguarding Lead (DSL): Mr Matt Farrah

Deputy Designated Safeguarding Lead(s): Ms Farah Khizar

Headteacher: Mr Paul Jones

School Address: Burlington House school Tooting, 3 Garrad's Road, London SW16 1JZ

Telephone 02081293890

Email: M.farrah@bhstooting.com

Where concerns indicate that a child may be at immediate risk of harm, staff should follow the school's Child Protection and Safeguarding procedures without delay.

Parents and carers who have concerns about a child's online safety are encouraged to contact the school as soon as possible.

15. Approval & Policy Review

This policy will be reviewed:

- annually;
- following significant safeguarding incidents where learning indicates amendments are required;
- following changes to statutory guidance;
- where technological developments introduce new safeguarding risks;
- following significant changes to the school's filtering and monitoring arrangements;
- following the annual Online Safety Risk Assessment.

The review will be led by the Central Team in partnership with the Board of Directors.

The Governing Body will receive assurance that:

- statutory requirements continue to be met;
- filtering and monitoring arrangements remain effective;
- emerging online risks have been considered;
- staff training remains current;
- lessons learned from safeguarding incidents have informed policy development.

The Governing Body will receive assurance that the school's online safety arrangements continue to reflect current statutory expectations and recognised good practice.

This Policy has been reviewed and approved by:

Policy Approver(s)	Cavendish Education Board of Directors/Senior Leadership Team of the school
Storage Location	Website, Online, hard copy in the schools
Effective Date	July 2025
Next Review Date	August 2027

16. Revision History

Version	Change	Author	Date of Change
1	First published	Cavendish Central Team	July 2025
2	Updated to bring in line with KCSIE 2026	Cavendish Central Team	September 2026
2.1	Updated to align with the Information Sharing Duty September 2026	Cavendish Central Team	2nd October 2026

17. Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers).

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:
Technology is an important part of learning at our school. This agreement explains how everyone can help keep themselves and others safe when using school technology. As a pupil, I agree that I will: **Use technology responsibly** • Use school technology, devices, networks and online services safely, responsibly and respectfully. • Use school technology for educational purposes unless a member of staff gives me permission to do otherwise. • Follow my teacher's instructions when using computers, tablets, laptops, mobile devices or other digital technology. • Respect other people when communicating or working online.

Keep myself and others safe
• Keep my usernames and passwords secure and never share them with anyone else.
• Protect my personal information and never share my full name, home address, telephone number, passwords or other personal details online without permission from a trusted adult.
• Tell a trusted adult immediately if:
  ○ I see anything online that worries, upsets or frightens me;
  ○ someone contacts me in a way that makes me feel uncomfortable;
  ○ I think another pupil may be at risk online;
  ○ I accidentally access inappropriate content;
  ○ I receive suspicious messages, emails or links.

Behave respectfully online I will: • be kind and respectful to others; • use appropriate language; • respect other people's privacy; • think carefully before posting or sharing anything online; • understand that my online actions can have consequences. I will not: • bully, threaten or deliberately upset anyone online; • share embarrassing, offensive or harmful content; • create or share fake accounts or impersonate another person; • share photographs, videos or recordings of other people without permission.
Use Artificial Intelligence (AI) responsibly Where AI tools are authorised by the school, I will: • use them only for learning purposes; • follow my teacher's instructions; • never use AI to bully, embarrass or harm another person; • never create or share AI-generated images or videos that could upset or exploit someone; • not submit AI-generated work as my own if this is against my teacher's instructions; • remember that AI can sometimes provide incorrect or misleading information.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Use the internet safely

I will not:

- access inappropriate websites or material;
- deliberately try to bypass the school's filtering or monitoring systems;
- download software or files without permission;
- open unknown email attachments or click suspicious links;
- arrange to meet anyone I have met online without the knowledge and permission of my parent/carer.

Look after school equipment

I will:

- look after school devices and equipment;
- report damaged equipment immediately;
- log off or lock devices when I have finished using them;
- only use equipment that I have permission to use.

Mobile phones and personal devices

If I bring a mobile phone or personal device into school, I will:

- follow the school's Mobile Phone Policy;
- keep my device switched off or stored securely during the school day unless a member of staff gives permission to use it;
- not use my device to photograph, film or record anyone without permission;
- not use personal devices to access inappropriate content or communicate inappropriately.

Filtering and Monitoring

I understand that:

- the school uses filtering and monitoring systems to help keep everyone safe online;
- my activity on school devices and networks may be monitored;
- if I do not follow this agreement, appropriate action will be taken in line with the school's Behaviour Policy and Online Safety Policy.

I understand how to use technology safely and responsibly and will follow these expectations whenever I use school technology.

Signed (pupil):	Date:

Parent/carer's agreement:

I understand that:

- technology is an important part of my child's education;
- the school uses filtering and monitoring systems to help safeguard pupils;
- my child is expected to use technology safely, responsibly and respectfully;
- I will support the school's expectations for the safe use of technology at home and at school;
- I will encourage my child to tell a trusted adult if they experience anything online that worries or upsets them;
- I will work with the school if an online safety concern arises;
- I understand that misuse of school technology or breaches of this agreement may result in appropriate safeguarding or disciplinary action.
- I have discussed this agreement with my child and will support them in following these expectations.

Signed (parent/carer):	Date:

18. Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Please see the full Policy - Acceptable Use Agreement (Staff) - 2024 Edition

19. Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

20. Appendix 5: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident