THE
KING'S SCHOOL
CANTERBURY

Online Safety Policy

Author: The Designated Safeguarding Lead

(DSL) Reviewer: Deputy Head, Pastoral

Publication Date: September 2026

Latest Review Completed: September 2026

Next Review Due: September 2028

TABLE OF CONTENTS

TABLE OF CONTENTS **2**

1. STATEMENT OF COMMITMENT **4**

2. PURPOSE **4**

3. LEGISLATIVE FRAMEWORK **4**

4. DEFINITION OF ONLINE SAFETY **5**

5. ROLES AND RESPONSIBILITIES **6**

5.1 The Governing Body 6

5.2 The Head 6

5.3 The Designated Safeguarding Lead (DSL) 7

5.4 All Staff 7

5.5 Pupils 8

5.6 Parents, Carers and Guardians 8

6. ONLINE RISKS **9**

6.1 Content 9

6.2 Contact 9

6.3 Conduct 9

6.4 Commerce 9

7. ARTIFICIAL INTELLIGENCE (AI) **9**

8. CHILD-ON-CHILD ABUSE ONLINE **10**

9. SHARING NUDE AND SEMI-NUDE IMAGES **11**

10. FILTERING AND MONITORING **12**

11. VIRTUAL PRIVATE NETWORKS (VPNS) **13**

12. CYBERBULLYING **13**

12. SOCIAL MEDIA **14**

12.1 Staff 14

12.2 Pupils 15

13. MOBILE DEVICES 15

13.1 External Listening and Recording Technology 16

14. VULNERABLE PUPILS 16

15. EDUCATION AND PREVENTION 17

16. REPORTING ONLINE SAFETY CONCERNS 17

17. REVIEW 17

1. Statement of Commitment

The King's School is committed to safeguarding and promoting the welfare of all pupils. We recognise that technology plays a significant role in children's lives and that online environments can present both valuable opportunities and significant safeguarding risks.

The School adopts a whole-school approach to online safety, recognising that online safety is a safeguarding issue and should be considered as a running and interrelated theme throughout safeguarding policies, procedures, curriculum delivery, staff training, pastoral support and leadership decision-making. Online safety is everybody's responsibility.

The School is committed to creating an environment where pupils, staff, parents and visitors can use technology safely, responsibly and positively whilst protecting themselves and others from harm. Staff must maintain professional curiosity when responding to online incidents.

2. Purpose

This policy aims to safeguard and protect all members of the school community when using digital technologies and online services. It establishes clear expectations for the safe, responsible, and acceptable use of technology, while supporting pupils in developing the digital resilience, critical thinking, and online safety skills needed to navigate the digital world confidently and responsibly.

The policy also ensures that staff are aware of emerging online risks and understand their responsibilities in identifying, responding to, and reporting concerns. Through promoting a culture of vigilance, openness, and timely reporting, the school seeks to ensure that online safety concerns are addressed promptly and effectively.

In doing so, the policy supports the school in meeting its statutory safeguarding duties and maintaining a safe and secure learning environment for all.

3. Legislative Framework

This policy should be read alongside:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- Children Act 1989 and 2004
- Education Act 2002
- UK GDPR
- Data Protection Act 2018
- Counter Terrorism and Security Act 2015
- Prevent Duty Guidance
- UK Council for Internet Safety (UKCIS) Guidance
- DfE Filtering and Monitoring Standards for Schools and Colleges
- Kent Safeguarding Children Multi-Agency Partnership (KSCMP) Procedures.

4. Definition of Online Safety

Online safety refers to the protection of children, young people and adults when using digital technologies, internet-connected devices, communication systems, applications, gaming platforms, social media and other online services. It encompasses both the safe use of technology and the safeguarding of individuals from harm that may occur through their online activity or interactions.

The School recognises that technology plays an important role in the lives of children and offers many educational, social and creative benefits. However, it also presents potential risks that can affect children's safety, wellbeing, mental health and development. As such, online safety is viewed as an integral part of the School's wider safeguarding responsibilities and is embedded throughout the curriculum, pastoral provision and safeguarding practice.

Online safety extends beyond the technical security of devices and networks and includes safeguarding concerns that may be facilitated, amplified or occur entirely through online environments, including:

- Child-on-child abuse.
- Cyberbullying and online harassment.
- Sexual harassment and sexual violence.
- Online grooming.
- Child Sexual Exploitation (CSE).
- Child Criminal Exploitation (CCE).
- Radicalisation and exposure to extremist material.
- Fraud, scams and financial exploitation.
- The impact of online activity on mental health and emotional wellbeing.
- Abuse, manipulation or exploitation facilitated through Artificial Intelligence (AI).
- The creation, sharing or possession of nude or semi-nude images and videos.
- Online coercion, control and blackmail.
- Exposure to harmful, inappropriate or illegal content.
- Discriminatory, hateful or prejudicial behaviour.
- Misinformation, disinformation and manipulated content.
- Risks associated with online relationships, gaming and livestreaming platforms.

The School recognises that online harms can occur at any time and may take place both within and outside the school environment. These harms may involve known individuals, strangers, organised groups or artificial intelligence technologies. Online risks can have a significant impact on a child's physical safety, emotional wellbeing, educational outcomes and wider development.

In line with the School's Safeguarding and Child Protection Policy and statutory safeguarding guidance, the School recognises that abuse and harm occurring online can be equally as serious as abuse occurring face-to-face. Concerns relating to online safety will therefore be identified, reported, assessed and responded to with the same level of seriousness and rigour as any other safeguarding concern. Staff will adopt a child-centred approach, taking account of the individual needs, vulnerabilities and experiences of the child involved, and will work with parents, carers and relevant agencies where appropriate to promote safe, responsible and positive use of technology.

5. Roles and Responsibilities

Online safety is a safeguarding responsibility shared by the entire school community. The School adopts a whole-school approach to online safety, recognising that effective safeguarding requires leadership, accountability, vigilance and collaboration at all levels.

5.1 The Governing Body

The Governing Body is responsible for ensuring that appropriate online safety arrangements are in place as part of the School's wider safeguarding framework. In carrying out this responsibility, the Governing Body will:

- Ensure that online safety is effectively embedded within the School's safeguarding culture and strategic planning.
- Ensure that appropriate filtering and monitoring systems are in place, regularly reviewed and effective in safeguarding pupils.
- Maintain strategic oversight of online safety, including emerging risks, trends and safeguarding requirements.
- Ensure that online safety policies, procedures and practices are reviewed and evaluated regularly.
- Seek assurance that safeguarding arrangements are operating effectively and that online safety concerns are identified and managed appropriately.
- Ensure that appropriate resources, staffing and training are available to support the School's online safety arrangements.
- Promote a culture in which pupils, staff and families understand the importance of safe and responsible technology use.

5.2 The Head

The Head has overall responsibility for the implementation of this policy and for ensuring that online safety forms an integral part of the School's safeguarding arrangements. The Head will:

- Promote and maintain a strong safeguarding culture in which online safety is recognised as everyone's responsibility.
- Ensure that online safety is embedded throughout the curriculum, pastoral systems and wider school life.

- Ensure that appropriate policies, procedures and reporting mechanisms are in place and implemented consistently.
- Provide sufficient resources to enable effective online safeguarding practice.
- Support the Designated Safeguarding Lead (DSL) in carrying out their responsibilities.
- Ensure that staff understand their safeguarding obligations and receive appropriate training and support.
- Foster positive relationships with parents, carers and external agencies to support online safety.

5.3 The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead is the strategic lead for online safety and has primary responsibility for coordinating the School's response to online safeguarding concerns. The DSL will:

- Lead and oversee the School's online safeguarding arrangements.
- Maintain an up-to-date understanding of online safety risks, emerging technologies and evolving safeguarding concerns.
- Work closely with relevant staff to understand and oversee the effectiveness of filtering and monitoring systems.
- Receive, assess, record and manage online safety concerns and incidents in line with safeguarding procedures.
- Ensure that online safety concerns are appropriately risk assessed and that suitable support is provided to those affected.
- Maintain accurate safeguarding records relating to online incidents and concerns.
- Liaise with parents, carers, safeguarding partners, the police and other agencies where appropriate.
- Provide advice, guidance and support to staff regarding online safeguarding matters.
- Coordinate staff training and awareness programmes.
- Review online safety procedures and contribute to the review of this policy.

5.4 All Staff

All staff have a responsibility to safeguard and promote the welfare of children, including protecting them from online harm. Staff must:

- Read, understand and comply with this policy, the School's Safeguarding and Child Protection Policy, Staff Code of Conduct and related procedures.
- Maintain an awareness of online safeguarding risks and emerging technologies.
- Promote safe, responsible and respectful use of technology.

- Model positive digital behaviour and professional online conduct.
- Remain professionally curious and alert to indicators of online abuse, exploitation or harm.
- Take all concerns seriously and report them promptly in accordance with safeguarding procedures.
- Contribute to a culture in which pupils feel listened to, respected and supported.

When responding to safeguarding concerns, staff should maintain the mindset that:

"It could happen here."

All concerns, regardless of how minor they may initially appear, should be considered with a safeguarding perspective and acted upon appropriately.

5.5 Pupils

Pupils play an important role in creating a safe and positive online environment. Pupils are expected to:

- Use technology and online services safely, responsibly and respectfully.
- Follow the School's Acceptable Use Policy and other relevant school expectations.
- Treat others with kindness, respect and consideration both online and offline.
- Protect their personal information and respect the privacy of others.
- Report online concerns, worries or incidents to a trusted adult as soon as possible.
- Engage positively with online safety education and guidance provided by the School.
- Contribute to a culture that challenges bullying, abuse, discrimination and harmful online behaviour.

5.6 Parents, Carers and Guardians

The School recognises that parents, carers and guardians play a vital role in supporting children to navigate the online world safely. The School will work in partnership with families by:

- Providing information, advice and guidance about online safety risks and safe technology use.
- Sharing information about emerging online safeguarding concerns and trends.
- Offering access to resources, training opportunities and support where appropriate.
- Encouraging effective supervision and age-appropriate boundaries for technology use at home.
- Promoting open communication between children and trusted adults about their online experiences.
- Working collaboratively with families when responding to online safety concerns affecting pupils.

By working together, the School aims to create a safe, inclusive and supportive digital environment where children can benefit from technology while being protected from online harm.

6. Online Risks

The School recognises that pupils and staff may be exposed to a range of online risks, which broadly fall into four categories: content, contact, conduct and commerce. The School is committed to identifying, managing and mitigating these risks through effective education, safeguarding practices, filtering and monitoring arrangements, and clear reporting procedures.

6.1 Content

These risks may include exposure to harmful, inappropriate or potentially distressing content, including pornography, violence, hate-based material, content that promotes or depicts self-harm or suicide, extremist material, and false or misleading information, including misinformation and disinformation.

6.2 Contact

This includes harmful interactions with others online, such as grooming, radicalisation, exploitation, sextortion, coercive behaviour, harassment, and other forms of abuse that may place a child at risk of harm.

6.3 Conduct

These risks may include behaviours conducted online that cause harm to others, such as cyberbullying, online abuse, sexual harassment, image-based abuse, the sharing of harmful content, impersonation, and other forms of inappropriate or abusive conduct.

6.4 Commerce

These risks may include online activities involving commerce and financial transactions, such as scams, fraud, gambling, loot boxes, financial exploitation, cryptocurrency-related fraud, and other practices that may result in financial loss or harm.

7. Artificial Intelligence (AI)

The School recognises that developments in Artificial Intelligence (AI) technologies present both opportunities and emerging safeguarding challenges. AI tools are increasingly accessible and can be used in ways that place children and adults at risk of harm, exploitation, abuse or misinformation.

AI-related safeguarding risks may include, but are not limited to:

- The creation or distribution of deepfake images, videos or audio recordings.

- AI-generated nude, semi-nude, sexualised or intimate images.
- Bullying, harassment, intimidation or humiliation through AI-generated content.
- Identity theft, impersonation and the creation of deceptive online profiles.
- The generation and dissemination of false, misleading or harmful information.
- Online grooming, sexual exploitation and coercive behaviour.
- Image-based abuse and non-consensual creation or sharing of content.
- Child-on-child abuse facilitated through the use of AI technologies.
- The manipulation of images, videos or audio to cause distress, reputational harm or emotional abuse.
- Exposure to inappropriate, harmful or unlawful AI-generated content.

The School will take all concerns relating to the misuse of AI technologies seriously. The creation, possession, sharing or use of AI-generated content that harms, humiliates, harasses, exploits or targets any individual will be treated as a safeguarding concern and responded to in accordance with the School's Safeguarding and Child Protection Policy, Behaviour Policy and associated procedures.

Pupils will be educated about the safe, ethical and responsible use of AI technologies, including how to recognise manipulated content, misinformation and potential online risks. Staff will remain vigilant to emerging AI-related safeguarding threats and will respond promptly to concerns.

Any suspected misuse of AI, including the creation or sharing of harmful, abusive, sexualised or deceptive content, must be reported immediately to the Designated Safeguarding Lead, who will assess the concern and take appropriate safeguarding action.

8. Child-on-Child Abuse Online

The School recognises that children can abuse other children online and that such behaviour may occur both within and outside of school. Online child-on-child abuse can have a significant impact on a child's safety, wellbeing and development and will be treated as a safeguarding concern. Consistent with the School's Safeguarding and Child Protection Policy and the principles of *Keeping Children Safe in Education 2026*, all concerns will be taken seriously, recorded appropriately and responded to promptly.

Online child-on-child abuse may include, but is not limited to:

- Cyberbullying, including prejudice-based and discriminatory bullying.
- Online sexual harassment.
- Sharing, creating or threatening to share nude, semi-nude or sexual images or videos without consent.
- AI-generated abuse, including the creation, manipulation or distribution of harmful, sexualised or degrading content.

- Deliberate exclusion, humiliation or intimidation.
- Coercive, controlling or exploitative behaviour.
- Threatening, abusive or harmful communications.
- Hate-related incidents and discriminatory behaviour.
- Encouraging or facilitating harmful, unsafe or illegal activities online.

The School adopts a zero-tolerance approach to all forms of child-on-child abuse. Staff will never dismiss abusive behaviour as "banter", "just having a laugh", "part of growing up" or "children being children". Reports will be assessed on a case-by-case basis, with the needs and safety of all children involved considered. Appropriate safeguarding action, support, risk assessment and, where necessary, referral to external agencies will be undertaken in accordance with the School's Safeguarding and Child Protection Policy.

9. Sharing Nude and Semi-Nude Images

The School recognises that incidents involving the sharing of nude or semi-nude images can be distressing and potentially harmful for all children involved. Such incidents will be managed in accordance with the School's Safeguarding Policy and current UK Council for Internet Safety (UKCIS) guidance on responding to incidents involving the sharing of nudes and semi-nudes.

The term "nudes and semi-nudes" refers to any image, video or live stream that shows all or part of a child's genitals, buttocks or breasts, or depicts a child in a sexualised manner. This may include content that has been created, shared, manipulated or generated using digital technologies, including Artificial Intelligence (AI).

The School recognises that the sharing of nudes and semi-nudes may occur for a range of reasons and that children involved may have been subjected to coercion, exploitation, abuse, peer pressure, grooming or manipulation. As such, all incidents will be approached in a child-centred, safeguarding-focused manner that prioritises the welfare, wishes and needs of the child.

Any concern relating to the creation, possession, viewing, distribution or sharing of nude or semi-nude images must be reported immediately to the Designated Safeguarding Lead.

Staff must not:

- View images unless there is a clear and justifiable safeguarding reason to do so.
- Copy, print, save, store or forward images.
- Request, encourage or pressure a child to share images.
- Share images with colleagues unless this forms part of an agreed safeguarding response.
- Use language or behaviours that could be perceived as blaming, shaming or judging the child.

When responding to a disclosure, staff should:

- Remain calm, supportive and non-judgemental.
- Reassure the child that they have done the right thing by speaking to a trusted adult.
- Explain what will happen next and who may need to be informed.
- Record the concern accurately and promptly in accordance with safeguarding procedures.
- Ensure the child's safety and wellbeing remain the primary consideration throughout the process.

All incidents will be carefully risk assessed and managed on a case-by-case basis by the DSL, taking account of the age, developmental stage, vulnerability and individual circumstances of those involved. Appropriate safeguarding measures, support and referrals to external agencies will be considered where necessary to protect children from further harm and to promote their welfare.

10. Filtering and Monitoring

The school's filtering and monitoring infrastructure includes:

- Securly which provides age-appropriate web filtering to prevent access to harmful online content.
- Fastvue Reporter which reports and analyses on network layer traffic passing through the school's firewall.
- Senso which provides real-time activity monitoring on school managed devices. Senso also generates alerts for concerning activity and behaviours.
- Prisma Browser which provides filtered web access and online behaviour reports.
- HTTPS Inspection which enables encrypted web traffic to be inspected so that inappropriate content, hidden within secure websites, can be identified and filtered.

Monitoring information is only accessed by authorised personnel for safeguarding, safeguarding investigations, information security, operational management, or compliance purposes, in line with the school's Data Protection, Acceptable Use, and Safeguarding policies.

Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection.

Filtering breaches will be reported to the DSL and will be recorded and escalated to technical staff as appropriate and in line with relevant policies.

Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material),

Kent Police, NCA-CEOP or Kent Integrated Children's Services via the Kent Integrated Children's Services Portal.

If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or management team.

11. Virtual Private Networks (VPNs)

The School recognises that Virtual Private Networks (VPNs) can have legitimate educational, business and security purposes. However, the use of VPNs may also enable users to bypass the School's filtering, monitoring and safeguarding systems, thereby increasing the risk of exposure to harmful content, inappropriate online activity, or unauthorised access to school systems.

The use of VPNs on School-owned devices, networks or systems is prohibited unless expressly authorised by the Head, Designated Safeguarding Lead (DSL), Network Manager or another designated senior leader for a legitimate educational, operational or security purpose. Pupils must not install, access or use VPN software, applications, browser extensions or proxy services to circumvent the School's filtering and monitoring arrangements.

Staff must not use personal VPN services on School devices or networks where doing so would interfere with the School's safeguarding, filtering, monitoring or information security processes. Any staff member requiring the use of a VPN for legitimate business purposes must obtain prior approval from the appropriate authorised individual and ensure that its use complies with the School's safeguarding, data protection and cyber security requirements.

The School reserves the right to monitor, investigate and restrict the use of VPNs or similar technologies where there is reason to believe that they are being used to bypass security controls, access inappropriate material, conceal online activity, or otherwise breach School policies. Any unauthorised use of VPNs by pupils or staff may result in disciplinary action and, where appropriate, further safeguarding or information security investigations.

The School's filtering and monitoring systems will be configured, where reasonably practicable, to detect and prevent the use of unauthorised VPNs, proxy services and other technologies designed to evade online safety controls. Any concerns regarding the use of such services must be reported promptly to the DSL and/or IT team in accordance with the School's safeguarding and online safety procedures.

12. Cyberbullying

The School is committed to providing a safe, respectful and inclusive environment for all pupils and will not tolerate cyberbullying. Allegations of cyberbullying will be taken seriously and addressed promptly and proportionately. Where cyberbullying places a child at risk of harm, it will be treated as a safeguarding concern.

Cyberbullying may include, but is not limited to:

- Sending abusive, offensive, intimidating or threatening messages.
- Deliberately excluding individuals from online groups, activities or communications.

- Creating fake accounts, impersonating others or sharing misleading content.
- Posting, sharing or encouraging harmful comments, rumours or allegations.
- Sharing, or threatening to share, images, videos or personal information without consent.
- Public humiliation, harassment or targeted online abuse.
- Creating, altering or distributing AI-generated or manipulated content intended to cause distress, embarrassment or harm.
- Any other behaviour that causes, or is intended to cause, physical, emotional or psychological harm to another person online.

The School will respond to incidents of cyberbullying in accordance with its Safeguarding and Child Protection Policy, Behaviour Policy and Anti-Bullying Policy. All reports will be investigated, appropriate support will be provided to those affected, and suitable action will be taken. Where necessary, concerns will be referred to external agencies. Cyberbullying may result in disciplinary measures in line with the School's Behaviour Policy

12. Social Media

The School recognises that social media can provide valuable opportunities for communication, learning and engagement. All members of the school community are expected to use social media responsibly, safely and respectfully, in a manner that reflects the School's values and safeguards the wellbeing of others.

12.1 Staff

Staff are expected to maintain the highest standards of professional conduct when using social media and online platforms. The use of social media by staff is governed by the School's **Staff Code of Conduct**, **Safeguarding and Child Protection Policy** and relevant employment policies.

Staff must:

- Always maintain clear professional boundaries with pupils.
- Not communicate with current pupils through personal social media accounts or platforms.
- Ensure that privacy and security settings on personal accounts are appropriately configured.
- Protect confidential, sensitive and personal information relating to pupils, families, colleagues and the School.
- Consider the potential impact of their online activity on their professional reputation and the reputation of the School.
- Report any safeguarding concerns, inappropriate online contact, or online incidents involving pupils in accordance with school procedures.

Any online conduct that breaches the Staff Code of Conduct, compromises safeguarding, or brings the School or the teaching profession into disrepute may be dealt with through the School's disciplinary procedures.

12.2 Pupils

Through the curriculum and wider safeguarding programme, pupils will be supported to develop the knowledge and skills needed to navigate the online world safely, responsibly and critically.

Online safety education will include:

- Understanding digital footprints and the long-term impact of online activity.
- Using privacy and security settings effectively.
- Safe and respectful online communication.
- Developing healthy and appropriate online relationships.
- Recognising, responding to and reporting online risks or concerns.
- Identifying misinformation, disinformation and manipulated content, including content generated using artificial intelligence (AI).
- Understanding the importance of consent, respect and responsible behaviour online.

Pupils are expected to use social media and online platforms responsibly and in accordance with the School's Behaviour Policy, Anti-Bullying Policy and Acceptable Use Policy. They are also expected to comply with the minimum age requirements of social media platforms and adhere to relevant legislation relating to online conduct. Any misuse of social media or online platforms that causes harm to others, compromises safety, or breaches school expectations will be addressed through the School's safeguarding, behaviour management and disciplinary procedures.

13. Mobile Devices

Pupils may bring mobile devices to school in accordance with the School's Mobile Phone Policy. Expectations for the possession and use of mobile devices are age-appropriate, reflect the needs of different year groups, and are aligned with current government guidance. Further information can be found in the School's Mobile Phone Policy.

Mobile devices must never be used to:

- Bully, intimidate, threaten or harass others.
- Create, access, possess or share harmful, offensive or inappropriate content.
- Take, store or distribute images, videos or recordings of others without their knowledge or consent.
- Share nude, semi-nude or indecent images.
- Facilitate child-on-child abuse, discrimination, exploitation or any other form of harmful behaviour.

- Circumvent school filtering, monitoring or safeguarding measures.

Any misuse of a mobile device that causes harm, breaches school expectations, or places a child at risk will be addressed in accordance with the School's Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy and Mobile Phone Policy, and may result in disciplinary action.

Staff may access School systems and resources using personal devices. However, staff must not use personal devices to communicate with pupils on platforms outside of the school's network except in exceptional circumstances where this has been expressly authorised and is consistent with the School's Staff Code of Conduct and safeguarding procedures. Any approved communication must be for a legitimate professional purpose, be transparent and professionally appropriate, and take place through methods that can be appropriately recorded, monitored and reviewed.

13.1 External Listening and Recording Technology

To safeguard the privacy, welfare, and safety of all members of the school community including academic integrity, the use of personal external listening, recording, monitoring, or surveillance devices is prohibited on school premises and during school activities unless expressly authorised by a member of SMT. This prohibition includes, but is not limited to, smart glasses with audio, video, or recording capabilities, wearable cameras, digital voice recorders, listening devices, and similar technologies.

14. Vulnerable Pupils

The School recognises that some children may be more vulnerable to online risks and may require additional support, monitoring or intervention to help keep them safe online. Staff will remain vigilant to the individual needs and vulnerabilities of pupils when assessing online safety concerns.

Children who may be at increased risk include, but are not limited to:

- Children with Special Educational Needs and Disabilities (SEND).
- Children who have a social worker.
- Children in care (Looked After Children) and previously looked after children.
- Children experiencing mental health difficulties or emotional wellbeing concerns.
- Children who are vulnerable to exploitation, including criminal or sexual exploitation.
- Children who may be isolated, experience discrimination, or face additional barriers in accessing support.
- Any child whose personal circumstances may increase their susceptibility to online harm.

The School adopts a child-centred approach to online safety and recognises that vulnerabilities may overlap and change over time. Where appropriate, additional safeguarding measures, targeted education, pastoral support, risk assessments and multi-agency involvement will be implemented to ensure that children receive the support they need to stay safe online.

15. Education and Prevention

Online safety education is embedded throughout the curriculum and wider pastoral programme, including Life Matters, Computing, assemblies, tutor time and safeguarding awareness activities. Through these opportunities, pupils are taught how to stay safe online, develop and maintain healthy relationships, understand the importance of consent, and recognise how and when to report concerns.

The School also promotes pupils' ability to think critically about online information, identify misinformation and manipulation, use artificial intelligence technologies safely and responsibly, and develop the digital resilience required to navigate an increasingly complex online world. This education is delivered in an age-appropriate manner and is designed to equip pupils with the knowledge, skills and confidence needed to make safe, informed and responsible choices online.

16. Reporting Online Safety Concerns

All staff have a responsibility to safeguard pupils and promote their wellbeing in both the physical and online environments. Any online safety concern, however minor it may appear, must be taken seriously and reported promptly in accordance with the School's safeguarding procedures.

Staff must report immediately to the Designated Safeguarding Lead (DSL) any concern involving a pupil's safety or welfare online, including but not limited to exposure to harmful content, online grooming, exploitation, cyberbullying, radicalisation, sextortion, harassment, inappropriate online contact, the sharing of nude or semi-nude images, or any behaviour that may place a child at risk of harm. Staff should not investigate incidents themselves beyond establishing the basic facts necessary to make an informed referral.

Concerns relating to the misuse of technology, breaches of the School's Acceptable Use Policy, cyber security incidents, attempts to circumvent filtering and monitoring systems, or access to inappropriate material should also be reported promptly to the DSL and/or the Director of IT as appropriate.

17. Review

This policy will be reviewed at least annually by the Headteacher, Designated Safeguarding Lead (DSL) and Governing Body to ensure that it remains effective, reflects current safeguarding practice, and complies with statutory guidance and legal requirements.

An earlier review may be undertaken in response to:

- Changes to legislation, statutory guidance or government expectations.
- Updates to *Keeping Children Safe in Education* or other relevant safeguarding guidance.
- Significant safeguarding incidents, online safety concerns or critical incidents.
- Changes to school procedures, technology, systems or online platforms used by the School.

- Findings from safeguarding audits, inspections, monitoring activities or risk assessments.
- Recommendations from the Local Authority, safeguarding partners or other relevant agencies.