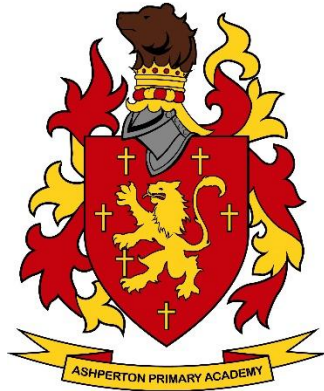




Ashperton Primary Academy Trust

SG43 On Line Safety Policy

Date of Last Review --New Policy Aug 2026

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Child-on-child sexual abuse and harassment
6. Grooming and exploitation
7. Mental health
8. Online hoaxes and harmful online challenges
9. Cyber-crime
10. Online safety training for staff
11. Online safety and the curriculum
12. Use of technology in the classroom
13. Use of mobile devices
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Artificial intelligence (AI)
20. Social networking
21. Ashperton Primary Academy Trust website
22. Use of devices
23. Remote learning
24. Monitoring and review

Appendix A: Online harm and risks – curriculum coverage

Appendix B: Ashperton Primary Academy – Local Online Safety Arrangements

Statement of intent

Ashperton Primary Academy Trust (APA) recognises that children must be safeguarded from potentially harmful and inappropriate online material. An effective whole-school approach to online safety empowers APA to protect and educate pupils and staff in their use of technology and establishes clear mechanisms to identify, intervene in and escalate concerns where appropriate.

Primary Academy Trust (APA) understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful content, e.g. pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories.
- **Contact:** Being subjected to harmful online interaction with other users or generative AI applications that simulate this, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Online behaviour that increases the likelihood of, or causes, harm, e.g. making, sending and receiving explicit images, including those generated using AI and online bullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. APA has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Children's Wellbeing and Schools Act 2026
- DfE 'Meeting digital and technology standards in schools and colleges – Filtering and monitoring: core standard'
- DfE 'Harmful online challenges and online hoaxes'

DfE (2026) 'Mobile phones in schools'

- DfE (2026) 'Keeping children safe in education 2026'

DfE (2026) 'Working Together to Safeguard Children 2026'

- DfE 'Teaching online safety in schools'
- DfE 'Searching, screening and confiscation'

DfE 'Generative AI: product safety expectations'

- DfE 'Generative artificial intelligence (AI) in education'
- Department for Digital, Culture and Media and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies and documents:

- Social Media Policy (HR15)
- Allegations of Abuse Against Staff Policy (SG5)
- Cyber-security Policy (F15)
- Cyber Response and Recovery Plan

- Child Protection and Safeguarding Policy and Procedures (SG1)

Online safety is reflected within SG1, including appropriate filtering and monitoring arrangements and the school's safeguarding response to online harm.

- Child-on-child Abuse Policy (SG10)
- Anti-Bullying Policy (SG19)
- Staff Code of Conduct (HR26)
- Behaviour and Restorative Practice Policy (SG48)
- Disciplinary Policy and Procedure (HR3)
- Data Protection Policy (F20)
- Pupil Confidentiality Policy (SG28)
- Photography and Images Policy (SG9)
- Staff ICT and Electronic Devices Policy (F16)
- Prevent Duty Policy (SG2)
- Remote Education Policy (CU18)
- Safe Use of AI Policy (SG27)
- Sharing of Nude or Semi-nude (Youth Produced Sexual Imagery) Policy (SG44)
- Social, Emotional and Mental Health (SEMH) Policy (SG21)
- Mobile Devices Policy (F23)

2. Roles and responsibilities

The Trust Board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.

- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant APA policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The Headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout APA's policies and procedures, including the Child Protection and Safeguarding Policy, curriculum, teacher training, parental engagement and safeguarding arrangements.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT support provider to conduct regular light-touch reviews of this policy.
- Working with the DSL and Trust Board to update this policy on an annual basis.
- Identifying and assigning roles and responsibilities to manage the APA's filtering and monitoring systems.
- Appointing an SLT digital lead in line with the Cyber-security Policy.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT provider.
- Ensuring online safety is recognised as part of APA's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the APA's approach to remote learning.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at APA and ensuring they continue to meet the school's safeguarding needs.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in APA's provision and using this data to update APA's procedures.
- Reporting to the Trust Board about online safety on a regular basis.
- Working with the Headteacher and ICT supplier to conduct regular light-touch reviews of this policy as required.
- Working with the Headteacher and Trust Board to update this policy on an annual basis.

ICT Provider will be responsible for:

- Providing technical support in the development and implementation of APA's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that APA's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Headteacher to conduct regular light-touch reviews of this policy as required.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of current and emerging online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with APA's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.

- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people. Staff will understand that pupils are at risk of abuse and other safeguarding concerns online as well as face to face, and in many cases, abuse will take place concurrently online and offline.

The DSL has overall responsibility for APA's approach to online safety, with support from deputies and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and Trustees receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted which include the topic of remaining safe online

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy and Procedures.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher, it is reported to the Chair of Trustees.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and ICT support provider, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour and Restorative Practices Policy and Child Protection and Safeguarding Policy and Procedures.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

APA will avoid unnecessarily criminalising pupils where behaviour is thought to be inadvertent and arises from age- or developmentally-appropriate curiosity, while recognising that making or sharing nudes and semi-nudes involving children is illegal and may be abusive. The DSL will assess each incident individually and manage it in line with the Child Protection and Safeguarding Policy and Procedures and SG44 Sharing of Nudes and Semi-Nudes (Youth Produced Sexual Imagery) Policy, involving the police or other agencies where appropriate.

All online safety incidents and APA's response will be recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

APA will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as lesbian, gay, bisexual, or gender questioning pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. Child-on-child sexual abuse and harassment

Pupils may use the internet and technology to facilitate child-on-child sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, offline and online, and that online elements may facilitate or accompany abuse that also occurs face to face.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual making or sharing of nudes and semi-nudes, including those generated or altered using AI.

For the purposes of this policy, images include photographs, videos and livestreams and may be self-generated, created by another person, digitally altered or wholly generated using AI, including deepfakes and deep nudes.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that making, possessing and sharing nudes or semi-nudes involving children is illegal, including where images have been digitally altered or wholly generated using AI, including deepfakes or deep nudes. Consensual image sharing, particularly between older children of the same age, may require a different safeguarding response and may not be abusive, but children must understand that it is illegal. Non-consensual making or sharing is abusive and illegal. All incidents will be managed in accordance with SG44 Sharing of Nudes and Semi-Nudes (Youth Produced Sexual Imagery) Policy and the Child Protection and Safeguarding Policy and Procedures.

APA will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. APA will respond to these incidents in line with the Child-on-child Abuse Policy, Child Protection and Safeguarding Policy and Procedures, and the Social Media Policy.

APA will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on APA premises or using APA-owned equipment. Concerns regarding online

child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy and Procedures.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways online. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production or distribution of child sexual abuse material (CSAM), or the sexual exploitation and trafficking of children.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting (including county lines activity), shoplifting, serious violence and other forms of criminal exploitation. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating online.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy and Procedures.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy and Procedures.

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand apps, games and websites, online terminology, the ways in which social interactions online in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an “**online hoax**” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online, e.g. via social media, game chats, and messaging platforms.

For the purposes of this policy, “**harmful online challenges**” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video online, e.g. through social media channels, and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff become aware of, or suspect, a harmful online challenge or online hoax that may pose a risk to pupils, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to APA or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.

- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy and Procedures.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

APA will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes online safety, including how the internet can facilitate abuse and exploitation and an understanding of the expectations, applicable roles and responsibilities relating to filtering and monitoring systems. All staff will be

made aware that pupils are at risk of abuse and other safeguarding concerns online as well as in person, and that, often, abuse and other risks will take place concurrently via online channels and in daily life. Online safety training will be provided at induction, regularly updated and reinforced through safeguarding updates at least annually.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum.

A progressive planned Online Safety education programme is delivered through discrete lessons and across the curriculum for all children in all year groups and is regularly revisited. Breadth

and progression are supported by the UKCIS Education for a Connected World framework and the school's use of Project Evolve.

APA's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as AI-generated content, deepfakes, pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Teaching will also address the prevalence and potential harms of deepfakes, pornography and misogynistic influencers, including how online content can influence attitudes, relationships and behaviour and when and where to seek help.

Contact risks

APA will educate pupils about the potential dangers of interacting with others online or generative AI applications that simulate this. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with making, sharing or receiving nudes and semi-nudes, including images that have been generated or altered using AI. Online bullying, including the use online platforms, e.g. social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of APA's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

APA will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy and Procedures.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy and Procedures.

12. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps, AI systems or other online platforms in the classroom, or recommending that pupils use these platforms at home, the teacher will review and evaluate the resource to ensure it is appropriate, safe and suitable for the age and needs of the pupils. Teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision will be suitable to their age and ability.

13. Use of mobile devices

While APA recognises that the use of mobile devices can have educational benefits, there are also a variety of associated risks which APA will ensure it manages.

APA will operate as a mobile phone-free environment by default. Pupils will not have access to personal mobile phones during the school day, including lessons, the time between lessons, breaktimes and lunchtime, except where an agreed exception applies. The arrangements will be managed in accordance with APA's Mobile Devices Policy.

Staff will use all personal technology in line with APA's Staff ICT and Electronic Devices Policy.

APA recognises that pupils may have access to the internet through personal devices and mobile phone networks outside the school day, or where school restrictions are circumvented. This can increase the risk of online behaviour that places pupils at risk of harm and breaches APA's Mobile Devices Policy and Technology Acceptable Use Agreement for Pupils.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the Behaviour and Restorative Practice Policy.

Inappropriate use of smart technology may include:

- Using mobile devices to sexually harass, bully, troll or intimidate peers.
- Making or sharing nudes and semi-nudes, including images generated or altered using AI, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

APA will hold assemblies, where appropriate, which address any specific concerns related to the misuse of technology and outline the importance of using technology in an appropriate manner.

APA will seek to ensure that it remains up to date with emerging technologies, including AI tools, devices, platforms, apps, trends and related risks.

APA will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

APA will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about APA's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Where pupils are asked to access online sites, platforms or services as part of school learning, parents and carers will be given appropriate information about what their child is being asked to do online and, where relevant, who from the school will be interacting with them online.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Making or sharing nudes and semi-nudes, including images generated or altered using AI.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online may be raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters

Clear escalation routes for parents/carers to raise online safety concerns with the school.

Parents/carers will be informed, where relevant, about what their child is being asked to do online, including the sites they may be asked to access and who from the school, if anyone, their child may interact with online.

Parents/carers will also be given information about the school's filtering and monitoring arrangements and how these contribute to keeping pupils safe.

- Online resources

15. Internet access

Pupils, staff and other members of the APA community will only be granted access to APA's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

All members of the APA community will be encouraged to use APA's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

The Trust Board will ensure APA's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's ['Filtering and monitoring standards for schools and colleges'](#). The Trust Board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

APA will do all it reasonably can to limit pupils' exposure to online risks from APA's ICT system. APA will put in place appropriate filtering and monitoring systems and ensure that their effectiveness is reviewed at least once every academic year and whenever there is a significant change to the school's network, safeguarding risks or technology provision. Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the DSL and ICT provider. Reviews will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record will be kept of these checks.

Monitoring systems will, where technically possible, allow activity to be traced to an individual user. Access to monitoring information and alerts will be restricted to authorised staff. Monitoring arrangements will be reflected in the school's privacy information and relevant data protection arrangements, including a data protection impact assessment where required.

The annual review will include checks that filtering and monitoring are working appropriately on all internet-connected devices in all relevant locations. APA will keep a record of the date of each check, who completed it, what was tested or checked, and any resulting actions.

Reviews will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record will be kept of these checks.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The Headteacher and ICT provider will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems APA implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

APA will consider the limitations of filtering and monitoring in relation to dynamic, personalised and AI-generated content and will take proportionate steps to mitigate identified gaps.

Requests regarding making changes to the filtering system will be directed to the Headteacher. Prior to making any changes to the filtering system, the ICT provider and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by the ICT provider. Reports of inappropriate websites or materials will be made to the ICT provider immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT provider, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour and Restorative Practice Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

APA's network and APA-owned devices will be appropriately monitored. All users of the network and APA-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy and Procedures.

17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by the ICT provider. Firewalls will be switched on at all times. The ICT provider will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to the ICT provider.

All members of staff will have their own unique usernames and private passwords to access APA's systems. Pupils in KS2 will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after a set number of days, after which users will be required to change them.

Users will inform the ICT provider if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL. Full details of the APA's network security measures can be found in the Cyber-security Policy.

18. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy, and Staff and Volunteer Confidentiality Policy.

Staff and pupils will be given approved APA email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail and report the email to the ICT provider. APA's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. APA will organise regular cyber awareness training, including guidance on recognising phishing emails, AI-generated phishing attempts and other malicious communications. This training will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

19. Artificial intelligence (AI)

APA will take steps to prepare pupils for changing and emerging technologies, including generative AI, and teach them how to use AI safely, responsibly and appropriately, taking account of their age and developmental stage.

APA will ensure its ICT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

APA will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

APA will take steps to ensure that personal, confidential or sensitive information is not entered into AI tools unless this is authorised, secure and compliant with data protection legislation.

Where staff use AI tools to support teaching, learning or administrative tasks, they will do so in accordance with APA's Safe Use of AI Policy and DfE guidance on generative AI in education.

APA will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Staff and pupils will be taught and reminded that AI-generated content can be inaccurate, misleading or harmful, and that AI can be used to create realistic manipulated or fabricated images, including deepfakes and deep nudes. Concerns involving AI-generated sexualised imagery will be managed in line with SG44 and SG1.

Where APA chooses to use generative AI, the school will consider the safety, safeguarding, data protection, ethical and intellectual property implications before use. Any pupil-facing AI tools will be age-appropriate and used in accordance with the age restrictions and safety requirements of the tool and relevant DfE guidance.

20. Social networking

The use of social media by staff and pupils will be managed in line with APA's Social Media Policy.

21. Ashperton Primary Academy Trust's website

The Headteacher will be responsible for the overall content of the APA website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website will be managed in line with APA's Website Policy.

22. Use of devices

Staff members and pupils will be issued with APA-owned devices to assist with their work, where necessary. Requirements around the use of APA-owned devices can be found in the APA's Device User Agreement.

The use of personal devices on APA premises and for the purposes of school work will be managed in line with the Staff ICT and Electronic Devices Policy and Pupils' Personal Electronic Devices Policy.

23. Remote learning

All remote learning will be delivered in line with APA's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

Where remote education is used, online safety arrangements will include appropriate platform selection, staff supervision, safeguarding reporting routes, clear expectations for pupil and staff behaviour, and communication with parents and carers about safe online participation.

24. Monitoring and review

APA will carry out an annual review of its online safety approach, supported by an annual risk assessment that considers and reflects the online risks faced by pupils, including emerging risks associated with new technologies and artificial intelligence. Findings will inform updates to this policy, curriculum, staff training and filtering and monitoring arrangements.

APA recognises that the online world is constantly changing; therefore, the DSL, the ICT provider and the Headteacher conduct regular light-touch reviews of this policy to evaluate its effectiveness.

The Trust Board, Headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is 31 August 2027.

Any changes made to this policy are communicated to all members of the school community.

25. Appendix A: Online harm and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	This risk or harm will be covered in the following curriculum areas: • Relationships and health education • KS2 Computing
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

	• What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	• Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	• Relationships education • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as ‘harvesting’ or ‘farming’. Teaching will include the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: • Health education • Computing

Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following: • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

	What acceptable and unacceptable online behaviours look like	
Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: - How to recognise extremist behaviour and content online - Which actions could be identified as criminal activity - Techniques used for persuasion - How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following: - What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal - How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why - That it is okay to say no and to not take part in a challenge - How and where to go for help - The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	This risk or harm will be covered in the following curriculum areas: Relationships education
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	• That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	• Relationships education
Fake profiles	Not everyone online is who they say they are. Teaching will include the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm will be covered in the following curriculum areas: • Relationships education
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they	This risk or harm will be covered in the

	do not know or have not met. Teaching will include the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	following curriculum areas: • Relationships education • Computing
--	--	---

Wellbeing

Impact: Quality of life Physical health Mental health Relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues	This risk or harm will be covered in the following curriculum areas: • Health education
---	--	--

	• That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm will be covered in the following curriculum areas: • Relationships education

Appendix B: Ashperton Primary Academy – Local Online Safety Arrangements

1. School Context

This appendix outlines the specific systems, procedures and practices in place at Ashperton Primary Academy to support the implementation of the Trust Online Safety Policy (SG43). It should be read in conjunction with the main policy.

2. Roles and Responsibilities (Local)

The Designated Safeguarding Lead (DSL) has overall responsibility for online safety and safeguarding.

The Online Safety Lead / Computing Manager is responsible for the day-to-day management of online safety, including filtering, monitoring and staff support.

The Safeguarding Governor oversees online safety as part of their safeguarding responsibilities.

Named roles are reviewed annually and recorded within safeguarding documentation.

3. Filtering and Monitoring Systems

Ashperton Primary Academy uses the following systems to ensure effective filtering and monitoring:

Filtering System: Securely (provided by Exa Networks)

Monitoring: Daily reports are generated and reviewed by the Computing Manager and/or DSL

Incident Logging: All online safety concerns are recorded using MyConcern

Procedures:

Alerts and reports are reviewed daily

Any safeguarding concerns are escalated immediately to the DSL

Inappropriate access attempts are investigated and recorded

Staff may request website access/unblocking through the Online Safety Lead, subject to appropriate checks and approval

4. Cyber Security and Data Protection

The school maintains robust cyber security measures, including:

Managed antivirus, anti-malware and anti-spam protection via Microsoft 365

Endpoint monitoring and threat detection using Huntress Managed Detection and Response (MDR)

Secure, encrypted backups:

Local encrypted backups

Offsite cloud-based backups

Access to systems is controlled through secure authentication processes, and staff are expected to follow Trust data protection and password policies at all times.

5. Teaching and Learning (Curriculum Implementation)

Online safety is embedded within the curriculum and wider school life through:

Use of Project Evolve to deliver a progressive online safety curriculum

Integration within Computing, PSHE and wider safeguarding curriculum

Regular assemblies, including focus events such as Safer Internet Day

Opportunities for pupil voice, including the use of Digital Leaders where appropriate

Pupils are taught:

Safe and responsible use of technology

How to recognise and report concerns

Age-appropriate understanding of online risks

6. Staff Training and Awareness

All staff receive regular online safety training as part of safeguarding updates.

Staff are informed of emerging risks, including those linked to new technologies and artificial intelligence.

Online safety guidance is shared through briefings and internal communication.

7. Working with Parents and Carers

The school actively engages parents and carers in supporting online safety through:

Newsletters and updates

Information shared via the school website

Parent meetings and workshops where appropriate

Guidance on supporting children's safe use of technology at home

Information about filtering and monitoring arrangements and how these contribute to keeping pupils safe.

Parents are encouraged to report any concerns to the school.

8. Responding to Online Safety Incidents

All incidents are managed in line with safeguarding procedures:

Concerns are logged on MyConcern

The DSL determines appropriate action

Where necessary, external agencies are involved

Use of Devices and Searching

In line with safeguarding guidance:

Staff may search devices where there is a safeguarding concern, in accordance with the Searching, Screening and Confiscation guidance and relevant school policies.

Staff will not intentionally view indecent images of children.

Devices may be secured and passed to appropriate authorities if required.

Content will not be deleted if it may be required as evidence.

All actions are recorded and reported to the DSL.

9. Local Safeguarding Procedures

The school follows local safeguarding partnership guidance and procedures, including those set by Herefordshire Local Authority.

Online safety concerns are treated as safeguarding concerns where appropriate.

10. Acceptable Use Agreements

The school uses Acceptable Use Agreements (AUPs) for:

Pupils

Staff

Parents/carers (where appropriate)

These agreements outline expectations for safe and responsible use of technology and are reviewed regularly. Copies are available from the school and/or published on the website.

Signed_____ Headteacher

Date_____

Signed_____ Chair of Trustees

Date_____