Online Safety and Social Media Policy

Date adopted: September 2026

Review Period: 1 year

Next review: September 2027

History of most recent policy reviews

Date	Review	Who is Responsible?
September 2023	**Updated with new statutory guidance**	**DSL**
September 2024	**Updated with new statutory guidance**	**DSL**
September 2025	**Updated with new statutory guidance and to reflect change to IT support**	**DSL**
September 2026	**Updated with new statutory guidance**	**DSL**

OFFICIAL

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 and smart technology
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Artificial Intelligence
20. Social networking
21. The school website
22. Use of devices
23. Data Protection
24. Remote learning
25. Monitoring and review

Appendices

A. Online harms and risks – curriculum coverage
B. Home School Agreement & Pupil Acceptable Use Agreement (KS2)
C. Pupil Acceptable Use Agreement (Foundation / KS1)
D. Parent/Carer Acceptable Use Agreement
E. Photographs and the Use of Digital / Video Images

OFFICIAL

Statement of intent

Air Balloon Hill Primary School 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 material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, 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. Our school 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.

OFFICIAL

1. Legal framework

This policy has due regard to all relevant legislation and 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 (2025) 'Filtering and monitoring standards for schools and colleges' DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024=5) 'Keeping children safe in education 2026'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2022) 'Searching, screening and confiscation'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Teaching online safety in school'
- DfE (2025) 'Generative artificial intelligence in education'
-

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

- Reporting Low-Level Concerns About Staff Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreements (Staff and Pupils)
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE scheme of work
- Relationships and Sex Policy and scheme of work
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Device User Agreement
- Prevent Duty
- Staff Use of ICT and Electronic Devices Policy
- Pupils' Personal Electronic Devices Policy

OFFICIAL

2. Roles and responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Lead's (DSL) 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 annually.
- Seeking assurance that there are appropriate filtering and monitoring systems in place.
- Seeking assurance 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 school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Identifying a link governor for safeguarding whose remit includes reporting on online safety measures and online safety issues at least twice a year.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the safeguarding team 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 annual safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- 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.
- Working with the DSL, IT Manager and governing board to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.

OFFICIAL

- 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 SENDCo and IT Support Services.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up to date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Understanding the filtering and monitoring processes in place at the school.
- 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 and ensuring they continue to meet the school's safeguarding needs.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- 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 the school's provision and using this data to update the school's procedures. Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Reporting to the governing board about online safety at least twice a year through the link governor's reports.
- Working with the headteacher and governing board to update this policy on an annual basis.

The school's IT Support Service is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that there are appropriate filtering and monitoring systems in place and are updated as appropriate.

All staff members are 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 the school's reporting procedure, including any occurrences of 'overblocking'.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are 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.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Social Media websites, in particular, ensuring that no images of children taken on the school premises or whilst on school trips or events are uploaded onto any social media sites (including Facebook and YouTube)

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet. 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 the school's approach to online safety, with support from other senior leaders 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 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, including via our Online Safety SKR (Safe, Kind and Respectful) Week.
- Assemblies are conducted on the topic of remaining safe online
- Conducting pupil surveys about their online habits, behaviour and experiences and sharing the findings, along with appropriate responses, with the relevant staff, governors and parents

OFFICIAL

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 Safeguarding Policy.

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, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, Reporting Low-Level Concerns About a Member of Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and IT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding and Child Protection Policy.

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

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. where a pupil has shared nudes or semi-nudes of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL. The outcome of any investigation will determine whether it is recorded as a behaviour incident or a safeguarding concern.

OFFICIAL

4. Cyberbullying

Cyberbullying can include 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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. TikTok, Instagram, YouTube, Snap Chat and Facebook
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school 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 also use the internet and technology as a vehicle for sexual abuse and harassment. All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. 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. and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

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. Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

Staff will be aware the school does not tolerate sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing

OFFICIAL

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 creating, possessing, and distributing nudes or semi-nudes involving other children, including images generated or altered using AI may constitute a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves. Such incidents will be handled in accordance with the Making or Sharing of Nude or Semi-nude Images Policy. The school 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. The school will respond to these incidents in line with the Safeguarding and Child Protection Policy.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

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, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer’s attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel ‘special’, particularly if the person they are talking to is older.
- 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.

OFFICIAL

- 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 through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking. 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 Safeguarding and Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process often happens online and 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. 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 Prevent Duty.

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.

OFFICIAL

Concerns about the mental health of a pupil will be reported to the school's Mental Health Lead, the Assistant Headteacher for Pastoral and Safeguarding, so that appropriate support can be offered.

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 social media 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 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 there may be a harmful online challenge or online hoax circulating amongst pupils in the school, 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 the school 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 Safeguarding and Child Protection Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, 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 even to individual children 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.

The school 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, and the school's IT Support Service will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

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 the school's Online Safety Curriculum, promoting a consistent, whole-school approach to digital safeguarding.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and the Safeguarding and Child Protection Policy.

11. Online safety and the curriculum

The school teaches an Online Safety Curriculum to all year groups, using the South West Grid for Learning 'Project Evolve' resources. There are six strands which are revisited during each year of school.

Term 1	Health, wellbeing & lifestyle: The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.
Term 2	Online Bullying: Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation
Term 3	Online Relationships: Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.
Term 4	Online reputation: Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles
Term 5	Privacy & security: Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.
Term 6	Managing online information: Strategies for effective searching, critical evaluation and ethical publishing

Online safety is also addressed in the following curriculum areas:

- School Assemblies
- SKR Weeks
- RSE
- PSHE
- Inquiry Projects
- ICT

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

OFFICIAL

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
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

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.

Contact risk

The school 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.

OFFICIAL

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 online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The DSL is involved with the development of the school'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.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND, CiC and pupils with a social worker. Relevant members of staff, e.g. the Assistant Headteacher for Inclusion and the Assistant Headteacher for Pastoral and Safeguarding, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL 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 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are 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.

OFFICIAL

During an online safety lesson or activity, the class teacher ensures 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 Safeguarding and Child Protection and Policy.

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 Safeguarding and Child Protection and Policy Use of technology in the classroom

12. Use of technology, including smart technology

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

- Computers and Computer Programs
- Laptops
- Tablets
- Internet
- 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 are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

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

Pupils will not be permitted to use personal mobile devices at any point during the school day unless exceptions apply. The prohibited use of personal mobile devices will be managed in accordance with the school's Pupil Electronic Devices Policy.

Staff will use all smart technology and any personal technology in line with the school's Staff Code of Conduct, Staff ICT and Electronic Devices Policy and the Staff Acceptable Use Agreement

The school 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 the school's Pupil Electronic Device policy and acceptable use of ICT agreement for pupils. Inappropriate use of smart technology may include:

- Using mobile and smart technology 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.

OFFICIAL

Pupils will not be permitted to use smart devices or any other personal technology whilst on the school site. Further information can be found in the Pupil Electronic Devices Policy.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour and Anti-bullying policies.

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

The school will seek to ensure that it remains up to date with emerging technologies, including AI tools, devices, platforms, apps, trends and related risks through staff training, local authority and safeguarding network updates, guidance from organisations such as the DfE, SWGfL and UK Safer Internet Centre, liaison with IT support providers, and regular review of safeguarding incidents and emerging themes.

Any safeguarding concerns involving AI tools, including misuse of generative AI, AI-generated imagery, deepfakes, inappropriate content creation or unsafe interactions with AI systems, will be recorded in accordance with the school's safeguarding procedures. The DSL will monitor incidents and emerging themes and report any significant trends to senior leaders and governors through existing safeguarding reporting arrangements.

The school will consider the 4C's (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.

13. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Acceptable Use Agreement when their child starts school and at the beginning of KS2. They are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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.

OFFICIAL

Parental awareness regarding how they can support their children to be safe online is raised through the schools' newsletter, the online safety pages of the school website and through parent presentations throughout the academic year.

14. Internet access

Pupils are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the school office.

15. Filtering and monitoring online activity

The governing body will ensure the school'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 governing 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.

The school will do all it reasonably can to limit pupils' exposure to online risks from the school's ICT system. The school will put in place appropriate filtering and monitoring systems and ensure that their effectiveness is reviewed at least annually 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 support from the DSL and IT technicians.

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 DSL and IT Support Service will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school 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.

The filtering and monitoring systems currently used by the school are set by the Local Authority IT Department. The IT Support Service undertakes termly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Any changes made to the system are recorded by IT Support Service Reports of inappropriate websites or materials are made to the DSL immediately, who investigates the matter and makes any necessary changes and where necessary will report it to the Headteacher or DSL.

OFFICIAL

Deliberate breaches of the filtering system are reported to the DSL, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour 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.

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

16. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the IT Support Service. Firewalls are switched on at all times. The IT Support Service. reviews the security systems on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are not to download unapproved software or open unfamiliar email attachments and are expected to report all malware and virus attacks to the IT Support Service.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils in Key Stage 2 are provided with their own unique username. Staff members and pupils are responsible for keeping their passwords private. Passwords expire after 90 days, after which users are required to change them.

Users inform the IT Support Service or School Business Manager. if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not 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 is informed and decides the necessary action to take.

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

17. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Confidentiality Policy.

Staff are given approved school email accounts and are only 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 must agree to and sign the Acceptable Use Agreement. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail and report the email to ICT technicians. The school'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. ICT technicians will organise **annual** 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 are managed in line with the Information Security Incident Policy

18. Social networking and the use of social media

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break and lunchtimes on their personal devices only; however, inappropriate or excessive use of personal social media during school hours may result in further action. The Code of Conduct makes clear the expectations that staff members must adhere to when using social media. Staff members are advised how any inappropriate conduct on social media can have an impact on their role and reputation within the school.

In addition to the expectations laid out in the Code of Conduct, staff must ensure that they:

- Communicate with children and parents in an open and transparent way using the school phone number and email address.
- Never ‘friend’ a pupil at the school past or present and under 18 years of age. If pupils attempt to ‘friend’ or ‘follow’ a staff member, they will report this to the headteacher.
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school’s reputation is compromised by inappropriate postings.
- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- Do not post any content online that is damaging to the school, its staff or pupils.
- Do not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.
- Do not post comments about the school, pupils, parents, staff or other members of the school community.

Staff are strongly advised to not ‘friend’ or ‘follow’ parents on their personal accounts.

OFFICIAL

In instances where there has been a breach of the school's Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.
- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Headteacher of the justification for any such action already taken or proposed.

The Headteacher will in turn seek advice from Bristol City Council where appropriate and may refer to external organisations for guidance. This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation.

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

19. Artificial intelligence (AI)

The school 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.

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

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI. The school 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 the school's Safe Use of AI Policy and DfE guidance on generative AI in education.

The school 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.

20 The school website

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

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the relevant consent has been provided by a pupil's parent or carer.

21 Use of devices

School-owned devices

Staff members may be issued with the following devices to assist with their work:

- Laptop
- Tablet
- Mobile Phone

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. laptops to use during lessons.

School-owned devices are used in accordance with the Device User Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

The IT Support Service. review all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT Manager.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

22. Personal devices

Personal devices – such as mobile phones – must be used in accordance with the Staff ICT and Electronic Devices Policy and the Pupils' Personal Electronic Devices Policy. Any personal electronic device that is brought into school is the responsibility of the user.

Staff members and visitors are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members and visitors are not permitted to use their personal devices to take photos or videos of pupils. Staff members and visitors should not allow pupils to use their personal devices.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy or Reporting Low-Level Concerns About a Member of Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

If a pupil needs to contact their parents during the school day, they should report to their teacher or the school office. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Pupils' devices can be searched, screened and confiscated in accordance with the Pupils' Personal Electronic Devices Policy and the Behaviour Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

23. Data Protection

Staff should not give their personal e-mail addresses to children or parents. Where there is a need for communication to be sent electronically the school e-mail address should be used. Likewise, staff should keep their personal phone numbers private and not use their own mobile phones to contact children or parents in a professional capacity.

There will be occasions when there are social contacts between children and staff, where for example the parent and teacher are part of the same social circle or staff are transport escorts. These contacts, however, will be easily recognised and openly acknowledged. Staff have a responsibility to make any such contact known to the senior leadership team.

Staff should never share their work logins or passwords with other people. Staff are advised to understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children.

OFFICIAL

Accessing, making and storing indecent images of children are illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Where indecent images of children are found by staff, the police should be immediately informed. Schools should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

Where other unsuitable material is found, which may not be illegal, but which raises concerns about that member of staff, Bristol City Council should be informed and advice sought. The school should not attempt to investigate or evaluate the material themselves until such advice is received.

24 Remote learning

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

25 Monitoring and review

The school recognises that the online world is constantly changing. The governing body, headteacher, DSL and IT manager review this policy in full on an annual basis or following online safety incidents.

The next scheduled review date for this policy is September 2027.

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

OFFICIAL

Appendix A: Online harms 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 includes 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 is covered in the following curriculum areas: • PSHE • Assemblies • Computing Online safety curriculum 'Privacy & security'
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes 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 is covered in the following curriculum areas: • Assemblies • PSHE/RSE education • Online Safety curriculum 'Managing online information' and 'Online reputation'
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following:	This risk or harm is covered in the following curriculum areas:

	• 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 • 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	• PSHE/RSE education • ICT lessons • Assemblies • Online Safety curriculum 'Managing online information'
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 includes 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 • 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	This risk or harm is covered in the following curriculum areas: • PSHE/RSE education • ICT lessons • Assemblies • Online Safety curriculum 'Privacy and security
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum areas: • Assemblies • Online Safety curriculum 'Privacy and security

Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • 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	This risk or harm is covered in the following curriculum areas: • ICT lessons Relationships education • Online Safety curriculum 'Privacy and security
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes 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 is covered in the following curriculum areas: • PSHE/RSE education • ICT lessons • Assemblies • Online Safety curriculum 'Privacy and security
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have	This risk or harm is covered in the

	planned or desired. Teaching includes 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 • How notifications are used to pull users back online	following curriculum areas: • Inquiry Projects (age appropriate) • Online Safety curriculum 'Privacy and security
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 includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum areas: • PSHE/RSE education • ICT lessons • Assemblies • Online Safety curriculum 'Privacy and security
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes 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 is covered in the following curriculum areas: PSHE/RSE education • ICT lessons • Assemblies • Online Safety curriculum 'Managing online information'
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in	This risk or harm is covered in the

	some cases, can be illegal. Teaching includes 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 • What acceptable and unacceptable online behaviours look like	following curriculum areas: • PSHE/RSE education • ICT lessons • Assemblies • Online Safety curriculum 'Online bullying
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • 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	This risk or harm is covered in the following curriculum areas: • RSE education • Online Safety curriculum 'Online bullying
Fake profiles	Not everyone online is who they say they are. Teaching includes 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 is covered in the following curriculum areas: • PSHE/RSE education • ICT lessons • Assemblies • Online Safety curriculum 'Online reputation'
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child	This risk or harm is covered in the

	sexual abuse and exploitation, and gangs and county lines. Teaching includes 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.	following curriculum areas: • PSHE/RSE education • Assemblies • Online Safety curriculum 'Online relationships'
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes 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	This risk or harm is covered in the following curriculum areas: • PSHE/RSE education • ICT lessons • Assemblies • Online Safety curriculum 'Online relationships'
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement	This risk or harm is covered in the following curriculum areas: • Assemblies

	• The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	• PSHE/RSE education • Online Safety curriculum 'Health, wellbeing and lifestyle
Impact on quality of life, physical and mental health and 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 includes 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 • 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	This risk or harm is covered in the following curriculum areas: • Assemblies • PSHE/RSE education • Online Safety curriculum 'Health, wellbeing and lifestyle
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives	This risk or harm is covered in the following curriculum areas: • Assemblies • PSHE/RSE education • Online Safety curriculum

	• How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	'Online relationships'
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum areas: • Assemblies • Online Safety curriculum 'Online reputation'
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	This risk or harm is covered in the following curriculum areas: • PSHE/RSE education (through healthy eating / mental health)

APPENDIX B – Home School Agreement & Pupil Acceptable Use Agreement (KS2)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS (KS2)	
Name:	**Class:**
When I use the school's IT systems (like computers) and internet at school I will: • Always use the school's IT systems and the internet responsibly and for educational purposes only • Only use them when a member of staff is present, and with their permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a member of staff immediately if I find any material which is not safe, kind or respectful • Always log off or shut down a computer when I'm finished working on it • Immediately report any damage or faults involving equipment or software, however this may have happened • Understand that information on the internet may not always be reliable and I should take care to check that the information that I access is accurate. I will not: • Access any inappropriate websites including social media or gaming sites unless my teacher has expressly allowed this as part of a learning activity • Access personal email accounts or instant messaging in school • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Download any software from the internet or access any materials which are illegal or inappropriate • Try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. Personal mobile phones and other personal electronic devices in school: • I know that if I walk to or from school unaccompanied by my parent/carer, I may bring a mobile phone into school. • I understand that this must be handed into my class teacher, school office or the Headteacher first thing in the morning to be locked away. • I understand that my phone remains my responsibility and is left at my own risk. • I understand that the online contents of my mobile phone may be searched by the school. • I know that if I use my mobile phone on the school site, it will be confiscated and my parent or carer will have to collect it from the Headteacher. • I will not take or distribute images of anyone without their permission.	
I understand that the school will monitor my use of the systems, devices and digital communications. I understand that I will only be allowed to use the internet if I use it responsibly and if I do not, I may not be allowed to use the internet at school. The school also has the right to take action against me if I am involved in incidents of inappropriate behaviour covered in this agreement.	
Signed (pupil):	Date:
Signed (parent/carer):	Date:

APPENDIX C - Pupil Acceptable Use Agreement (Foundation / KS1)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS (EYFS/KS1)	
Name:	**Class:**

At Air Balloon Hill Primary School, we believe that pupils have the right to safe internet access at all times. We ask parents of children in Reception and Key Stage 1 to discuss the points below with their child regarding online safety.

This is how we stay safe when we use computers:

- Children must ask a teacher or trusted adult if they want to use the computers
- Children will only use activities that a teacher or suitable adult has told or allowed them to use.
- Children will take care of the computer and other equipment
- Children will ask for help from a teacher or suitable adult if they are not sure what to do or if they think they have done something wrong.
- Children will tell a teacher or trusted adult if they see something that upsets them on the screen.
- Children know that if they break the rules, they might not be allowed to use a computer.

Signed (pupil):	Date:

Parent / Carer Countersignature

I have discussed the above points with my child and agree to them being allowed to use the computers and internet whilst at school

Signed (parent/carer):	Date:

APPENDIX D - Parent/Carer Acceptable Use Agreement

Parent/Carer Acceptable Use Agreement	
Pupil name:	Class

This Acceptable Use Policy is intended to ensure that:

- young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. Parents/carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Photographs/Video Images

Air Balloon Hill Primary School respectfully requests that Parents/carers refrain from using mobile phones in the playground so that their motives cannot be misinterpreted due to the sensitivities regarding the photographing of children. However, we recognise that there are many circumstances where a parent or carer will wish to take photographs or video images of their child at school events.

In order to comply with GDPR we invite parents/carers to inform us if they do not wish their child to be filmed or photographed completing the Photograph Consent Forms on Arbor or in Appendix E

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act).

To respect everyone's privacy and in some cases protection:

- Images taken on the school grounds must not be published/made publicly available on social networking sites (for example Facebook).
- Parents/carers must not comment on any activities involving other pupils in the digital / video images.
- We would expect other parents to report anything that they see on social media sites or online that they are unhappy about, including photographs of children at the school or other material which is detrimental to the school or individual children. This should be reported to the Headteacher, and we may, in turn, report the matter to the Police.

It is expected that parents/carers taking photographs or video images at school events will abide by the above guidelines. Any parent/carer found to be uploading images taken at school events or sharing those images with others will be asked to take down the images and may be requested to meet with the Headteacher and Chair of Governors and/or may be banned from any future school events or from the school site.

Declaration and Permission Form

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

• I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy. • I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety. • I have read and discussed the Online Safety and Social Media Policy and Acceptable Use Policy Agreement with my child and agree to support the school's policy. • I have read the above information about the taking of photographs/video images at school events, and I agree to abide by the guidelines. I understand that any breach of these guidelines may result in me being banned from attending future school events. • As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.	
Signed (parent/carer):	Date:
Signed (parent/carer):	Date:

APPENDIX E - Photographs and the Use of Digital / Video Images

During the course of their school life, there will be occasions where we would like to take photographs of pupils for use in displays in the classroom and/or in areas of the school which are on public display, on the school website, school YouTube channel or in school brochures or other printed materials authorised by the school in order to promote the school and the achievements of pupils in an appropriate way. There will also be times where we would like to take photographs or make video recordings of children for school projects. Parents and Carers should be aware that, photographs displayed on the school website or YouTube channel, may be disseminated worldwide.

There will also be lots of events in school at which parents/carers will want to take photographs or record video images of their children performing.

In addition, we may also be approached by members of the media wanting to take pictures or record film footage of our pupils in connection with activities such as productions, concerts, or other activities taking place at the school. Publicity can be of great benefit in the wider recognition it offers for the achievements of children at the school. We would therefore like to be able to offer the media the chance to take pictures and film where this is appropriate.

We recognise that there may be circumstances where a parent or carer will not wish their child to be filmed or photographed. We are therefore inviting you to give us your consent for the use of your child's photograph by filling in this form and returning it to the school. If you tick 'No', that's not a problem and we will accommodate your preferences.

Any photographs or video images taken by parents, carers or family members on the school site or as part of a school-led activity (e.g. a school WOW event) are done so in good faith and for personal use only. Images must NOT under any circumstances be posted on or uploaded to the internet and, in particular, to social media or networking sites such as Facebook.

We would like your consent to take and use your child's photographs in the ways described above. Please read the statements below and tick either Yes or No to indicate if you give your consent.

Under the UK's General Data Protection Regulations, from May 2018, consent cannot be inferred through silence or inactivity and therefore, if we do not receive a completed form from you, we have to assume that you do not give your consent for the taking and use of photographs and therefore will have no choice but to withdraw your child from the event or activity at which photographs are being taken.

It is intended that the preferences you indicate below will remain in place throughout your child's time at Air Balloon Hill Primary School, however, if you change your mind at any time, you can update your preferences by emailing the Data Manager - airballoonhillp@bristol-schools.uk

PHOTOGRAPH CONSENTS		
I give consent to my child's photograph being used on the school website	**A**	
I give consent to my child's image being used in videos that are published on the school YouTube channel	**B**	
I give consent to my child's photograph being included in public displays around the school.	**C**	
I give consent for my child's image to be used in Learning Records / Journals belonging to other children.	**D**	
I give consent to my child's photograph being used in printed school literature	**E**	
I give consent for my child's photograph to be used in the press (local or national)	**F**	
I give consent to my child appearing on TV or being included in radio programmes in connection with the school. We will always try to inform parents in advance if any filming is to take place in school	**G**	
I give consent for my child to participate in events at school, at which photographs and video images are being taken by other parents/carers Including, but not limited to, events such as Class Assemblies, May Day celebrations, the Nativity Play and Sports Days	**H**	
I give consent for my child to have an official school photograph taken. I understand in the case of class or year group photographs, printed/digital copies can be downloaded or purchased by other parents.	**I**	
I agree that any photographs or video footage that I take at school events will NOT be uploaded to the internet or posted on any social media or networking sites - including Facebook and YouTube	**J**	
NOTES ON CONSENTS:		

Signed: _____ **Date:** _____

Parent/Carer of: _____ **Class:** _____