POLICY

For

E-Safety

September 2016	September 2020	September 2023
January 2018	September 2021	September 2024
January 2019	September 2022	October 2025

'Striving for excellence, caring for all within a loving and caring Christian environment.'

We are a community in which everyone is offered the opportunity to fulfil their full potential, to understand themselves and be valued for who they are. Through a stimulating and challenging learning environment, we pursue academic excellence and seek the flourishing of all. This is because we know we are all God's children.

"Do all the good you can, by all the means you can, in all the ways you can, in all the places you can, at all the times you can, to all the people you can, as long as you ever can." John Wesley

"And as you wish that others would do to you, do so to them."
Luke 6:31

Article 4: The government has a responsibility to make sure your rights are protected. They must help your family to protect your rights and create an environment where you can grow and reach your potential.
Article 13: You have the right to find out things and share what you think with others, by talking, drawing, and writing or in any other way unless it harms or offends people.
Article 15: You have the right to choose your own friends and join or set up groups, as long as it isn't harmful.
Article 17 - Children have the right to get information. Adults should make sure that the information children are getting is not harmful, and help them find and understand the information they need.
Article 29: Your education should help you use and develop your talents and abilities. It should also help you learn to live peacefully, protect the environment and respect other people.
Article 34 - Children have the right to be free from abuse.
Article 36 - Children have the right to protection from any kind of exploitation.
Article 36: Every child has the right to be protected from doing things that could harm them.

Contents of E-Safety Policy:

1. **Rationale**
2. **Context and background**
3. **Roles and Responsibilities**
4. **Filtering and Monitoring and Cybersecurity**
5. **E-Safety for Pupils**
6. **E-Safety Curriculum**
7. **Use of the Internet by pupils**
8. **Safeguarding and Preventing Radicalisation**
9. **Use of the Internet and ICT by AAT staff**
10. **Responding to Online Safety Concerns**
11. **Data protection**
12. **Use of Ai**
13. **Courses for all school staff**

Appendix 1 – E-Safety Log

Appendix 2 - Types of incidents Guidance

Appendix 3 - Letter to parents/carers - pupil and parent/carer expectations

Appendix 4 – Reception/KS1 Pupil Acceptable Use Expectations

Appendix 5 – KS2 Pupil Acceptable Use Expectations

Appendix 6 – Parent/ Carer E-Safety Home/School Expectations

1. Rationale

Abbey Academies Trust recognises its fundamental duty to ensure that every child in our care is safe, both within our physical environment and in the increasingly complex digital world. As technology becomes ever more embedded in children's daily lives, the same principles of protection, care, and respect that guide our safeguarding practice in school must extend seamlessly to all online and digital contexts.

The purpose of this policy is to establish a comprehensive framework that safeguards and empowers all members of the Abbey Academies Trust community—staff, pupils, volunteers, governors, parents/carers and visitors—by promoting a safe, responsible, and inclusive online culture. This approach ensures that everyone who engages with Abbey Academies Trust's digital technologies, whether on-site or remotely, understands their role in keeping our community safe online.

Our Trust is committed to a whole-school and whole-community approach to online safety. This means every stakeholder—leaders, staff, pupils, and families—shares responsibility for modelling and maintaining safe and respectful online behaviour. Staff and governors play a pivotal role in embedding this culture, ensuring that our online safety practice reflects our shared ethos and statutory safeguarding duties.

At the heart of our online safety practice is our commitment to teaching children how to keep themselves safe, make responsible choices, and build digital resilience. This includes developing the skills, confidence, and critical awareness needed to recognise, respond to, and recover from online risks.

Our approach is underpinned by Abbey Academies Trust's values and the 3Rs:

- Respect and take care of ourselves
- Respect and take care of each other
- Respect and take care of our environment

These values, embodied in our mission statement "Striving for excellence, caring for all within a loving and caring Christian environment," guide our digital conduct and underpin our commitment to fostering integrity, empathy, and responsibility—both online and offline.

Abbey Academies Trust acknowledges that online safety is an essential aspect of safeguarding and a shared responsibility. We affirm our statutory duty to protect all learners and staff from online harm while recognising that digital technology also offers immense opportunities for creativity, learning, collaboration, and global connection.

This policy aims to:

- Promote a consistent culture of online safety, setting clear expectations for all Abbey Academies Trust community members' online behaviour and use of digital technologies.
- Support effective safeguarding practice by strengthening collaboration between safeguarding leads, curriculum teams, IT specialists, and senior leadership.

- Ensure that online conduct standards apply beyond the school gates, maintaining the same expectations of behaviour, integrity, and respect in both digital and physical spaces.
- Empower learners and staff to use technology safely, responsibly, and positively, preparing them for life and work in a connected world.
- Provide clear procedures for responding to online safety incidents, supporting a swift, proportionate, and restorative response.
- Abbey Academies Trust affirms that online safety is not only about protection—it is about education, empowerment, and preparing our children to flourish safely and confidently in a digital society.

2. Context and Background

The Digital Landscape
Information and Communication Technology (ICT) has a pervasive influence on all aspects of life in the 21st century. From communication and collaboration to creativity and innovation, technology plays a central role in the way children and adults live, learn, and interact. While the online world offers significant opportunities for learning and connection, it also presents a range of potential risks that must be carefully managed within the school environment and beyond.

Abbey Academies Trust recognises that online safety is not solely about protection—it is about preparation and empowerment. We aim to help children build the skills, confidence, and digital literacy required to thrive safely and responsibly in a connected world.

Balancing Opportunity and Risk
Despite the risks associated with being online, Abbey Academies Trust recognises the immense educational, social, and creative benefits that digital technology offers to children and young people. Technology is an integral part of adult life, and developing digital competencies from an early age is essential for future success and wellbeing.

The use of technology within our academies is always driven by pedagogy and inclusion. Decisions about digital tools and platforms are guided by educational value, accessibility, and safeguarding principles. For example, for younger children, we place a strong emphasis on guided and scaffolded learning experiences, limiting passive consumption (e.g., unrestricted scrolling) and promoting purposeful, creative engagement. Technology is used to support differentiation, accessibility, and inclusion, ensuring that all learners, including those with SEND, can participate fully and meaningfully.

Online Risks
Children encounter a range of online risks that can broadly be grouped into four categories:

- Contact: Risks arising from interactions with others online, such as grooming, bullying, coercion, harassment, or commercial exploitation (e.g. tracking and harvesting of personal data).
- Content: Exposure to inappropriate or harmful material such as violent, extremist, or pornographic content; misleading or biased information; or unwanted marketing and spam.
- Conduct: Risks relating to a child's own online behaviour, such as cyberbullying, illegal downloading, hacking, gambling, or sharing inappropriate content.
- Commerce: Risks from online advertising, phishing, scams, and fraudulent content.

Understanding these categories helps staff, pupils, and parents identify, manage, and mitigate online harms effectively.

Whole-Academy Approach
A safe and supportive digital learning environment across Abbey Academies Trust is founded on three key principles:

- Effective systems and technology – secure, age-appropriate hardware, software, and filtering/monitoring systems.
- Clear policies and responsibilities – well-defined roles and procedures to ensure accountability and consistency.
- Embedded education – a curriculum that empowers pupils to make safe, responsible, and ethical decisions online.

Online safety is not limited to computing lessons; it is threaded throughout the curriculum and across all aspects of school life. All staff share responsibility for identifying opportunities to reinforce online safety messages in context—whether during lessons, homework tasks, enrichment activities, or informal interactions.

Curriculum Design and Pedagogy

Abbey Academies Trust follows a carefully sequenced online safety curriculum that builds knowledge, skills, and competencies progressively across all key stages. This curriculum develops pupils' ability to understand online risks, make informed decisions, and apply their learning to real-world contexts.

In line with Teaching Online Safety in Schools guidance, we adopt a whole-school approach, embedding digital resilience, wellbeing, and critical thinking into everyday teaching and learning. This includes equipping staff to support pupils in recognising misinformation, managing online relationships, protecting privacy, and understanding digital footprints, data law, and copyright.

To ensure that teaching is effective, regular assessment and review take place through curriculum audits, self-evaluations, and pupil progress tracking. Tools such as diagnostic quizzes or reflective exercises may be used to identify where additional support or targeted intervention is needed.

The teaching of online safety is explicitly delivered through:

- Relationships, Sex and Health Education (RSHE/PSHE)
- Computing
- PSHE curriculum (through the Jigsaw scheme) and cross-curricular themes

However, all staff are expected to model safe, respectful online behaviour and to reinforce key messages wherever technology is used. When overseeing the use of technology—whether internet searches, online collaboration, or use of AI tools—staff must ensure that learning activities are age-appropriate, safe, and aligned with safeguarding expectations. This includes promoting critical evaluation of content, awareness of misinformation and disinformation (as emphasised in KCSIE 2025), and responsible participation in online communities.

Framework and Curriculum Alignment
Abbey Academies Trust aligns its digital education and online safety teaching with the UK Council for Internet Safety (UKCIS) framework: Education for a Connected World (2020 edition). This framework provides clear, age-appropriate competencies across key stages (EYFS–KS3 and beyond), supporting progression in understanding online relationships, media literacy, privacy, and digital identity.

Annual reviews of curriculum planning and schemes of work are carried out as part of curriculum team monitoring.

Statutory Framework

- Online safety teaching within Abbey Academies Trust is guided by statutory requirements including:
- The National Curriculum for Computing, which requires pupils to use technology safely, respectfully, and responsibly.
- The Relationships Education, RSE and Health Education (RSHE) Guidance, which ensures children learn the principles of healthy and respectful relationships, both online and offline.
- Keeping Children Safe in Education (2025) and Prevent Duty Guidance, which underpin our safeguarding practice and staff responsibilities.

Engagement with Parents and Carers

Partnership with parents and carers is vital in promoting consistent messages about online safety and digital wellbeing. Abbey Academies Trust communicates regularly with families about online safety through:

- Sharing this policy and curriculum overview
- Including updates in newsletters and parent workshops/webinars
- Providing links to age-appropriate resources and guidance
- Offering signposting to support materials

Through these measures, we ensure that our pupils are supported by a community that understands both the risks and opportunities of the online world and works collectively to keep them safe.

3. Roles and Responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

The following section outlines the online safety roles and responsibilities of all stakeholders across the online community within Abbey Academies Trust.

Headteacher/Head of School

The Headteacher holds overall responsibility for ensuring that online safety is embedded within the school's wider safeguarding culture, in line with statutory guidance and best practice.

The Headteacher must:

- Foster a whole-school culture of safeguarding, where online safety is recognised as an essential part of pupil wellbeing and protection.
- Support and oversee the work of the DSL and safeguarding team, ensuring collaboration with Ark to complete regular online safety audits and reviews.
- Undertake training in both online and offline safeguarding, following national and local guidance.
- Ensure all staff receive safeguarding training, including online safety, at induction and through regular updates, and that all staff adhere to relevant policies and procedures.
- Ensure governors and trustees receive regular safeguarding training, including online safety, and are kept informed of school practices and effectiveness.
- Oversee the implementation of safe and appropriate ICT systems, including secure email, remote access, and effective filtering and monitoring that meets DfE standards.

- Understand and review filtering and monitoring decisions, working with the DSL and Ark to ensure the rationale behind what is blocked/allowed is in line with safeguarding priorities.
- Receive regular updates from the DSL on online safety issues, incidents, and wider policy developments.
- Take overall responsibility for data management and information security, ensuring safeguarding needs are prioritised within data protection practices.
- Ensure all staff understand reporting procedures for serious online safeguarding incidents.
- Ensure the school website meets statutory requirements for safeguarding and information.
- Promote online safety across all areas of school life, ensuring it is included in policies, training, reporting, and curriculum planning.
- Ensure appropriate filters and monitoring systems are in place and regularly reviewed.
- Ensure robust reporting channels are available for pupils and staff to raise online safety concerns.
- Remind staff that their online conduct outside of school can impact their professional responsibilities and role.

Computing and E-Safety Lead Responsibilities
In addition to the expectations set out for all staff, the Computing and E-Safety Leads have key responsibilities in ensuring a whole-school approach to online safety.

They must:
- Oversee the delivery of the online safety elements of the Computing curriculum in line with the National Curriculum.
- Work collaboratively with the RSHE Lead to ensure online safety coverage is complementary, not duplicated.
- Liaise closely with the DSL and SLT to align messaging, ensure consistency in practice, and support the safeguarding agenda.
- Develop and review the school's E-Safety Curriculum annually to ensure it remains relevant, age-appropriate and up to date.
- Support a consistent approach to online safety by working with technical staff and others responsible for ICT and device use.
- Promote a whole-school culture of online safety, embedding it across the curriculum and school life.
- Ensure staff are aware of how to recognise, respond to and report online safety concerns, including procedures for doing so.
- Provide online safety training to staff at least annually, or more frequently in response to changes in legislation or emerging risks.
- Maintain personal knowledge and training in all matters relating to online safety and digital safeguarding.
- Review and update online safety policies, including Acceptable Use Policies, and submit these to SLT for approval (Appendix 4, 5 and 6)
- Provide clear guidance and accessible resources for staff, pupils, and parents to support safe online behaviours.
- Ensure children are taught to use the internet responsibly and understand how to keep themselves safe online.
- Communicate regularly with parents and carers, highlighting the importance of online safety at school and at home.
- Lead or contribute to the school's annual online safety review, feeding into safeguarding and curriculum planning.

Governors/Trustees
Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to risks from the school's IT system.

As part of this process, the academy Governing body should:

- Oversee and review all school policies, including the E-Safety policy.
- Regularly reviewing and evaluating the effectiveness of the filtering and monitoring systems in place - each school as an assigned filtering and monitoring governor.
- Ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- Consider how online safety is planned into the curriculum including teacher training, the role of the DSL (and deputies) and any parental engagement.

Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (Deputy DSL)

The DSL holds overall responsibility for safeguarding, including online safety, as outlined in *Keeping Children Safe in Education (KCSIE)*. While certain online safety duties may be delegated, this accountability cannot be transferred.

The DSL must:

- Lead on all safeguarding matters, including online safety, and ensure a whole-school approach is in place.
- Ensure children are taught to use the internet safely and responsibly through curriculum and wider school life (e.g. RSHE).
- Ensure all staff (including supply) and governors receive safeguarding and online safety training at induction and through regular updates — including filtering, monitoring, and child-on-child abuse.
- Support and monitor staff in understanding their responsibilities and ensure they have read relevant parts of KCSIE (Part 1 and Annex B).
- Stay up to date with online safety trends, risks and statutory guidance — including Prevent awareness training.
- Work with SLT, E-Safety Leads, Ark and governors to:
    - Monitor and review the school's filtering and monitoring systems.
    - Document filtering decisions and log incidents.
    - Ensure filtering meets DfE standards.
    - Complete regular online safety audits.
- Collaborate with the Executive Administrator and leadership to ensure safe, legal and appropriate data handling in support of safeguarding.
- Ensure online safety education is embedded throughout the curriculum using resources such as the UKCIS *Education for a Connected World* framework.
- Provide staff with clear procedures to follow in case of online safety incidents — including how to report and log concerns, both on- and off-site.
- Regularly communicate with SLT and the safeguarding governor, reviewing safeguarding trends, incidents, and system effectiveness.

School Staff

All staff must sign the Staff Acceptable Use Policy (AUP) and adhere to this E-Safety Policy, the school's Safeguarding Policy, the Staff Code of Conduct, and relevant sections of *Keeping Children Safe in Education (KCSIE)*.

Staff must:

- Report any online safety concerns—no matter how minor—to the Designated Safeguarding Lead (DSL).
- Maintain awareness of current online safety risks and guidance.
- Model safe, responsible, and professional use of technology, avoiding fear-based or victim-blaming language.
- Be aware of DfE filtering and monitoring standards, and report any overblocking, gaps, or attempts to bypass systems to the DSL.
- Supervise pupils' use of devices during lessons or school activities.

All school staff—including teaching and non-teaching roles—share responsibility for online safeguarding and must:

- Promote and model safe technology use.
- Follow all school policies related to online safety and safeguarding.
- Recognise, respond to, and report signs of online abuse or harm.
- Understand and follow referral and reporting procedures.
- Complete appropriate safeguarding and online safety training.
- Act in the best interests of pupils at all times.
- Maintain professional conduct and boundaries, both online and offline.
- Take responsibility for their own professional development in online safety.
- Sign the ICT Safeguarding (including Social Networking) agreement annually.

Class teachers must introduce and regularly reinforce the school's E-Safety Code (see Appendix 4 and 5) with pupils at the start of each school year.

Pupils

Read, understand, sign and adhere to the pupil acceptable use policy (Appendix 4 and 5)

Parents/Carers

Parents and carers need to understand the risks that children face online to protect them from online dangers. Parents need to:

- Read and adhere to all relevant policies.
- Be responsible when taking photos/using technology at school events.
- Know who the school DSL is.
- Know how to report online issues.
- Support online safety approaches and education provision.
- Be a role model for safe and appropriate behaviour.
- Identify changes in children's behaviour that could indicate they are at risk of online harm, abuse or exploitation.
- Read the parents/carers E-Safety home/school expectations (appendix 6)
- Read through the pupil acceptable use expectations with their child/children and support where appropriate.

4. Filtering and Monitoring and Cybersecurity

Academy Internet provision
The academy uses an Internet Service Provider, KCom, as part of Schools' Broadband consortium. KCom provides an always-on broadband connection at speeds up to 100 MB.

Content filter
The academy uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the Trust's Policy and Agreement for ICT Safeguarding (including Social Networking).
- School iPad usage history cannot be deleted on an individual device so that staff can track which websites children have accessed.

Downloading files and applications
The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of academy equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.
- App store/book store is switched off.

Portable storage media
Staff are allowed to use their own portable media storage (USB Keys etc.) however they must be password protected, this is in line with the GDPR Policy. If use of such a device results in an anti-virus message they should remove the device and immediately report to ARK.

Security and virus protection
The school subscribes to the recommended antivirus software program, Avast Antivirus software. The software is monitored and updated regularly by the system management company, ARK.

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to ARK.

5. E-Safety for pupils

Abbey Academies Trust is committed to equipping all pupils with the knowledge, skills, and confidence to navigate the online world safely, respectfully, and responsibly. Our aim is to help every child become a thoughtful and resilient digital citizen who can make positive choices, recognise potential risks, and know where to seek help when needed.

We believe that online safety education is most effective when it empowers pupils rather than restricts them. Therefore, pupils are encouraged to:

- Develop critical thinking skills to question and evaluate online information and media.
- Understand how to manage digital identity, privacy settings, and personal data securely.
- Recognise and respond appropriately to online bullying, unwanted contact, or suspicious behaviour.
- Explore positive and creative uses of technology while understanding the consequences of inappropriate or unsafe online conduct.
- Build resilience when encountering online challenges such as peer pressure, misinformation, or harmful content.

Children are taught how to report concerns through trusted adults in school, the Designated Safeguarding Lead (DSL), or recognised online reporting systems such as CEOP or Report Harmful Content.

Digital responsibility and respect are promoted across the curriculum and in everyday school life. Pupils are regularly reminded that the same values that guide their behaviour in person—respect, kindness, and integrity—apply equally in the digital space.

6. E-Safety Curriculum

At Abbey Academies Trust, we believe it is our responsibility to prepare pupils for their lives in a modern, digital world. Technology and ICT are integral to learning, communication, and creativity. We are committed to teaching pupils to use technology effectively, responsibly, and safely in all aspects of their education.

Use of the Internet by Pupils

Internet access is carefully monitored and controlled by staff according to pupils' age, experience, and learning objectives. Pupils are always actively supervised by an adult when using iPads, computers, or any device with internet access.
All browsing histories are visible to staff and cannot be deleted, allowing appropriate monitoring and follow-up.

Access for All Pupils

In line with our inclusion principles, all pupils should have equal access to technology that enhances learning. During periods of remote learning, we ensure that, as far as possible, pupils have the resources and devices they need to continue their education safely. If Internet-enabled devices are needed during after-school provision, supervision and clear expectations for safe use applies.

Using the Internet for Learning

The internet is a valuable tool for enquiry, exploration, and creativity. It is used across the curriculum for research, investigation, and digital learning. Teachers plan all online learning carefully to ensure that pupils access age-appropriate, reliable, and relevant material.
As part of the Computing Curriculum, pupils learn to:

- Use search engines effectively and critically evaluate digital information.
- Distinguish between commercial and non-commercial sites and identify the purpose and credibility of content.
- Recognise bias, misinformation, and persuasive techniques.
- Understand and respect copyright and ownership of digital materials, including text, images, and media.

Pupils use the digital learning platform Seesaw to upload, record, and share their learning. This platform empowers pupils to take ownership of their digital portfolios while maintaining strict privacy and security protocols.

Parents and carers receive weekly guides and termly newsletters with advice on online safety and practical tips for applying parental controls at home.

Teaching Safe and Responsible Use

Our e-safety curriculum is underpinned by the UKCIS "Education for a Connected World" framework, which equips children and young people with the knowledge and skills to thrive in a digital society. The framework covers eight key themes:

1. Self-image and identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing, and lifestyle
7. Privacy and security
8. Copyright and ownership

Each theme is taught progressively across all key stages and revisited regularly through monthly e-safety lessons alongside Computing. Lessons are designed to build understanding, awareness, and resilience as pupils mature.

Children are taught to:

- Evaluate what they see online and identify persuasive or manipulative content.
- Recognise online risks and know when and how to seek help.
- Manage their digital behaviour and privacy.
- Apply the 'Zip it, Flag it, Block it' code to help keep themselves and others safe online.
- Identify trusted adults and appropriate reporting routes including school staff, the police, Click CEOP, Childline, and Report Harmful Content.

National College / National Online Safety

Abbey Academies Trust is a proud member of the National Online Safety (NOS) platform, provided by The National College.
This partnership supports our whole-school approach by providing:

- Certified online CPD for all staff, governors, and parents/carers.
- Specialist training for DSLs, deputy DSLs, and SENDCos.
- Monthly webinars on current and emerging online issues.
- Weekly parental guides ("Wake Up Wednesday") on trending apps, games, and platforms, shared via our websites and social media.
- Curriculum-linked resources for EYFS, KS1, and KS2 aligned with the Education for a Connected World framework.

Through this collaboration, our staff remain up to date with DfE guidance and statutory expectations within Keeping Children Safe in Education.

Involvement of Pupils

Pupils play an active role in promoting e-safety within the Trust. Each class elects an E-Safety Champion, who attends meetings with the E-Safety Team, contributes to assemblies and Collective Worship, and helps share messages about online safety with peers.
E-Safety Champions wear identifiable badges to signify their leadership role and to encourage open, positive conversations about online behaviour.

7. Use of the internet by pupils

Suitable and Non-Educational Material

We encourage pupils to see the internet as a rich, creative, and educational resource. Staff provide pupils—especially younger ones—with recommended safe websites and ensure that any site used in lessons is checked for suitability.
Pupils also have opportunities to explore child-friendly educational and entertainment websites during supervised club sessions or at home, fostering responsible digital

independence.
Links to appropriate learning and recreational resources are available on each academy's website.

Responding to Unsuitable or Distressing Material

Despite strong filtering and supervision, pupils may occasionally encounter inappropriate or distressing content. Pupils are taught to report such incidents immediately to an adult.

When this occurs, staff will:

- Record the website or app involved and any linked content.
- Inform the DSL or a member of SLT.
- Log the incident in the E-Safety Log if applicable (Appendix 1).
- Relevant member of staff will discuss the incident with the pupil to support understanding and future prevention.

Social Networking and Online Communication

We recognise that pupils increasingly engage with online social platforms, particularly outside of school. Through lessons and assemblies, pupils learn about:

- Privacy and consent when sharing images or personal information.
- The risks and benefits of social networking, messaging, and online gaming.
- Strategies for managing their digital footprint and reputation.
- E-Safety Champions help promote safe use of social media and messaging platforms through peer discussion and pupil voice initiatives.

Mobile Phones and Handheld Devices

We acknowledge the potential benefits of mobile technology but also recognise the risks associated with unrestricted access.

Pupils in Years 5 and 6 may bring a phone for use on their journey to and from school. Devices must be switched off and handed to the teacher on arrival.

Mobile phones and similar devices are not permitted for use during the school day or at Kids' Club.

Pupils are taught about the legal and ethical implications of sharing personal information or images online and how data protection and privacy laws apply.

Cyberbullying

Cyberbullying includes any form of online harassment, intimidation, or harmful communication via digital means.
Pupils are taught how to recognise, report, and respond to all forms of online abuse.
Preventive strategies include:

- No access to public chatrooms, instant messaging, or open forums.

- Clear rules on mobile phone use and social media.
- Regular discussions and support resources for pupils and families.

All incidents are handled according to our Behaviour and Anti-Bullying Policy, with safeguarding concerns referred in line with child protection procedures.

Sanctions for Misuse

We share E-Safety Expectations with all pupils and pupils follow the school's E-Safety Code. Inappropriate use of technology or internet access results in proportionate sanctions, including restricted access, parental contact, or in serious cases, referral to senior leadership or external agencies.

Handling Complaints and Breaches

Any e-safety concerns or complaints are dealt with promptly and sensitively, following safeguarding procedures.
All incidents are logged and reviewed by the Designated Safeguarding Lead.
Serious breaches or staff-related concerns are escalated to the Head of School and CEO/Executive Headteacher.

8. Safeguarding and Preventing Radicalisation

We are committed to ensuring that our pupils are offered a broad and balanced curriculum that aims to prepare them for life in modern Britain. We encourage our pupils to be inquisitive learners who are open to new experiences and are tolerant of others. Our values support the development of pupils as reflective learners within a safe, respectful and tolerant learning environment. Through our curriculum, pupils are encouraged to share their views and recognise that they are entitled to have their own different beliefs which should not be used to influence others. Throughout the curriculum and, in particular within Computing, pupils are taught about how to stay safe when using the internet and encouraged to recognise that people are not always who they say they are online. Our curriculum responds to developments within technology and pupils are taught how to stay safe when they are using the internet. For example, they are taught that people are not always who they say they are, that information available on the internet can be misinformation, disinformation (including fake news) and how to spot scams. They are taught to seek adult help if they are upset or concerned about anything they read or see on the internet.

Extremists use the internet including social media, to share their messages. The filtering systems used in our school block inappropriate content, including extremist material, but pupils are regularly reminded to report any inappropriate material that may get through the school's filtering system.

9. Use of the Internet and ICT resources by AAT staff

Professional Use of the Internet

Abbey Academies Trust recognises that the internet is an invaluable resource for school staff. It provides access to a wealth of teaching materials, professional resources, research, and networks that support curriculum planning, professional development, and collaboration across the Trust and with external organisations.

Staff are encouraged and supported to use the internet to enhance teaching and learning, and to engage in professional dialogue and knowledge sharing. All internet use must reflect the school's professional and safeguarding expectations, and staff are expected to model safe, responsible, and inclusive ICT practice always.

Internet Availability

To support professional practice, internet access is available to all staff across the school. Staff should use this resource responsibly and in accordance with school policies, including the ICT Safeguarding and Acceptable Use Policy.

ICT Equipment and Resources

Staff are provided with access to a range of ICT equipment and resources to support teaching and learning, including:

- Computers, laptops, and iPads
- Interactive whiteboards
- Control and data-logging equipment
- Professional and curriculum software

Staff who require support or training to use ICT effectively in their professional practice can seek guidance from the Computing Team or request targeted INSET sessions.

Email

All staff are provided with a school email address for professional communication. Staff must use this email account for all official communication with colleagues, organisations, and external agencies.

Staff are reminded that:

- Their email use represents the school, and professional standards are expected in all communications.

- Occasional access by school management may be required for safeguarding, operational, or compliance reasons, while respecting personal privacy.

Online Discussion Groups, Bulletin Boards, and Forums

Engagement with professional online communities, discussion boards, and bulletin boards is encouraged to share best practice, participate in continuing professional development, and disseminate resources.

Staff must ensure that:

- Posts and messages are professional and appropriate.
- They are mindful that they represent Abbey Academies Trust and uphold its values and reputation.
- Personal opinions are clearly distinguished from official school communications.

Social Networking

Many staff use social networking platforms in their personal lives. Staff must remain aware of how their use of social media can impact their professional role. Guidance on social networking is provided in the ICT Safeguarding (including Social Networking) Policy and Staff Agreement, which outlines:

- Safe use of social media in both personal and professional contexts.
- Expectations for confidentiality, safeguarding, and professional conduct online.
- The importance of maintaining boundaries between personal accounts and professional responsibilities

10. Responding to Online Safety Concerns

The safety of the child and young person is of paramount importance. Immediate action may be required to safeguard investigations and any other children and young people. Any concern that children and young people may be at risk of harm, abuse or exploitation must immediately be reported to the DSL.

Online safety is recognised as part of the education settings safeguarding responsibilities – the DSL should take lead responsibility for online safety concerns which should be recorded and actioned. Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns. The child protection policy for Abbey Academies Trust includes procedures to follow regarding online safety concerns.

Staff should use Appendix 2 when dealing with an E-Safety incident. This document provides guidance on how to proceed with different types of incidents. Staff must remember if the incident is safeguarding to always go to a member of the Safeguarding Team and not the E-Safety Leaders.

Staff are responsible for documenting E-Safety incidents on the incident logs (more guidance is provided in Appendix 2).

As a Trust we are also aware of the impact of cyber security attacks upon education settings. '*Good cyber security protects that ability to function, and ensures organisations can exploit the opportunities that technology brings. Cyber security is therefore central to an organisation's health and resilience' (National Cyber Security Centre).*

School staff are trained and informed how to respond to potential cyber security threats, further information of which can be found in our *Cyber Security Policy.*

11. Data Protection

The school has a data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

Staff and pupils understand the legal and disciplinary implications of using the internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the internet by members of the school community using the connection provided by the school.

12. Use of Ai

As Generative Artificial Intelligence (Gen AI) continues to advance, AAT recognises its growing role in education. AI can support learning, teaching and school operations, but its use must always be safe, ethical and responsible, with safeguarding of staff and learners remaining our highest priority.

AAT acknowledges both the opportunities and risks of AI. Benefits include enhanced teaching and learning, improved outcomes, streamlined administration, reducing staff workload, and preparing staff and learners for a future where AI is integral. Risks will be

managed through existing policies and procedures, adapted as necessary to reflect emerging guidance.

Please also refer to the AAT Data Protection Policy regarding the use of Ai at AAT.

To guide safe and responsible use of AI, AAT commits to the following principles:

- **Curriculum**: Learners will be supported to understand how AI works, its benefits, risks and ethical/social impacts. AI literacy will be embedded where appropriate to help prepare pupils for future education and employment.
- **Data Protection and Security**: All AI use must comply with UK GDPR and AAT's data security standards. Only school-approved AI tools may be used, and staff must use school-provided accounts. Sensitive or confidential information must never be entered into unapproved third-party tools.
- **Accountability and Oversight**: Staff remain professionally responsible for all work involving AI. AI is a support tool, not a replacement for professional judgement. All AI-generated content must be checked for accuracy, reviewed for bias, and clearly marked as AI-assisted where appropriate. Final decisions that affect people will always be made by humans.
- **Transparency and Fairness**: Staff must be open about the use of AI and its limitations. AI must never be used in ways that discriminate, exclude or harm individuals or groups based on characteristics such as age, gender, ethnicity, race, disability or religion.
- **Reporting**: Any incidents of AI misuse, data breaches or inappropriate outputs must be reported immediately through safeguarding and IT channels, enabling prompt action and risk mitigation.
- **Professional Use**: Staff must seek permission before using AI for purposes such as transcribing, recording or analysing meetings, or processing personal data. AI tools may be used to support efficiencies in lesson planning, assessment and administration, provided they are approved and used responsibly.
- **Approved Tools**: AAT will maintain and publish a list of approved AI solutions. Only these may be used for school-related purposes to ensure compliance with safeguarding and data security requirements.

Through this approach, AAT will ensure that AI is used responsibly and positively, helping staff to work more efficiently, pupils to learn more effectively, and the Trust to prepare all members of its community for a future in which AI will play an increasingly important role.

13. Courses for all school staff

Abbey Academies Trust is committed to ensuring that all staff, governors, and other adults working within the Trust are fully equipped to safeguard pupils in the digital environment. Staff development in online safety is an essential part of this commitment.

As part of the Trust's National Online Safety (NOS) membership, all staff have access to a range of role-specific online safety courses. Completion of these courses results in a nationally recognised certificate, and courses are refreshed annually to reflect emerging technologies, risks, and statutory guidance.

Annual Online Safety Courses

Staff and governors undertake the following courses in line with their roles and responsibilities:

- **Teaching Staff:** Annual Certificate in Online Safety for Teaching Staff
- **SENDCOs:** Annual Advanced Certificate in Online Safety for SENDCOs

- **Computing/E-Safety Leaders:** Annual Advanced Certificate in Online Safety for ICT Leads
- **Safeguarding Team (DSLs and Deputy DSLs):** Annual Advanced Certificate in Online Safety for DSLs and Deputy DSLs
- **Wellbeing Officers:** Annual Certificate in Online Safety for Mental Health Leads
- **Governors:** Annual Certificate in Online Safety for School Governors
- **Non-Teaching Staff:** Annual Certificate in Online Safety for Support Staff

Course Content

The NOS courses cover a comprehensive range of topics, including:

- Current online risks and emerging technologies
- Safe and responsible use of devices, apps, and online platforms
- Remote learning safeguarding considerations
- Staff roles and responsibilities in protecting children online
- Practical strategies for promoting digital resilience in pupils
- Policy, procedures, and statutory compliance, aligned with *Keeping Children Safe in Education (2025)*

Monitoring and Record-Keeping

The Trust's E-Safety Team monitors staff engagement with these courses and maintains records of:

- Completed certificates
- Renewal dates for annual courses
- Additional role-specific training needs

Impact

This structured CPD programme ensures that all staff are confident and competent in identifying and managing online risks, supporting pupils in safe and responsible technology use, and maintaining the Trust's high standards of safeguarding across all digital contexts.

Appendix 1 *Found in policy*

E-Safety Log

Abbey Academies Trust
E-Safety Incident Log

All E-Safety incidents must be recorded and the E-Safety/safe guarding team must be notified. This incident log will be monitored and reviewed regularly by the Head of School and E-Safety Leaders.

Date of Incident:	Reported By:	Reported to:
Details of Incident: *You must include:* • Location • Type of concern (Cyber bullying/harassment/Bypassing security/inappropriate content/racist, sexist or homophobic material/radicalisation or extremism/material of a sexual nature/other		

Actions:	
Further Actions/Next Steps:	
Signed:	
Name:	
Date:	

Appendix 2

Types of incidents with guidance on what to do

An alert is received through the monitoring system.

1. The alert is received by one of the nominated members of the safeguarding team who will assess the risk as an alert may be triggered by a false positive
2. The safeguarding team will endeavour to identify the individual child who has accessed the site. Currently, this is done manually through a search of an ipads search history, the ipad having been identified as being in use at the time
3. Assess whether there has been intention behind the child's actions and respond to accordingly in line with policies which may include the Acceptable Use Policy, the Behaviour Policy, the Child Protection and Safeguarding policy

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety leaders and decide whether to inform parents of any children who viewed the site.
3. Inform Ark and ensure the site is filtered.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify SLT, parents of the child and E-Safety leads.
3. Inform Ark and ensure the site is filtered if need be.
4. Fill in E-Safety log.

An inappropriate website is accessed intentionally by a staff member.

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform Ark and ensure the site is filtered if need be.
5. In an extreme case where the material is of an illegal nature:
    a. Contact the local police and follow their advice.

An adult uses School ICT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.

2. Report the misuse immediately to the head teacher or a member of the safeguarding team and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the device to a secure place.
   - Instigate an audit of all ICT equipment by Ark to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (undertaken by Headteacher).
   - Inform governors/trustees of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police and follow their advice.
   - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to SLT.

Appendix 2 cont.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including E-Safety, anti-bullying, Child Protection and Safeguarding and PSHE and apply appropriate sanctions.
3. Inform the sender's e-mail service provider if known.
4. Notify parents of all the children involved.
5. Inform SLT.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection, LGFL)
9. Fill in E-Safety Log.

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform SLT.

2. Inform and request the comments be removed if the site is administered externally.

3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us

4 Endeavour to trace the origin and inform police as appropriate.

5. Inform Local Authority and other agencies (child protection, Governing body etc.).

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child.

1. Report to and discuss with a member of the Safeguarding Team in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.
7. Fill in an E-Safety log.

You are concerned that a child is playing computer games that are inappropriate or certificated beyond the age of the child.

1. Report to and discuss with a member of the E-Safety team (if you have no safeguarding concerns).
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that Ark block access to the game
4. Seek advice and support for parents e.g. Wake Up Wednesday Guides.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child.

1. Report to and discuss with a member of Safeguarding team in school and contact parents.
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that Ark block access to the game
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.
6. Discuss with E-Safety Leads to seek advice and support for parents e.g. Wake Up Wednesday Guides.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Discuss with SLT.
2. Contact the poster or page creator and discuss the issues in person
3. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
4. Contact governing body and parent association
5. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head of school and E-Safety Leads, who will keep the Executive Head Teacher informed.

Appendix 3
Letter to Parents/Carers

Dear Parents/Carers,

As part of your child's curriculum and the development of computing skills, our Trust provides supervised access to the internet. We believe that the use of the Internet is an essential skill for children as they grow up in the modern world. However, it is also essential that children do this in a responsible and safe way.

Although there are concerns in every school about children having access to inappropriate material via the internet, our Trust takes a range of measures to minimise these risks. We have a monitoring system in place which allows members of staff to check the material being searched for on the internet. We also have strict filtering in place to restrict the material which can be searched for by children.

In addition to this, children are educated on the safe and responsible use of the internet following 3 simple steps 'Zip it, Flag it, Block it'

Zip it- Keep your personal information private and think about what you say and do online.

Flag it- Tell someone you trust if anything upsets you or if someone asks to meet you offline. Think about your safe hands.

Block it- Block people who send nasty messages and don't open unknown links and attachments.

We are also part of 'National Online Safety' as we believe in taking a whole school community approach to keeping our children safe online. Each week we share a different 'Wake Up Wednesday Guide' on our school Facebook pages and on the school website. These guides provide advice and support for parents/carers on different apps and platforms.

Please read the attached E-Safety Home/School Expectations. Additionally, we ask that you read through the Acceptable Use Expectations (Reception and KS1 and/or KS2) with your child so that they understand what is appropriate and acceptable in our school. These will be fully discussed at school. I am sure you will agree that it is really important that all children, even those in Reception, understand the expectations of them when using the internet and that learning about and following some simple 'rules' from a young age can help children stay safe online.

Additionally, please see our policy for Parental Use of Social Networking and Internet sites on the school website. Paper copies can be requested from the school office.

By working together, we hope that we can educate children in how to stay safe when using the internet.

If you have any questions, do not hesitate to contact me.

Yours sincerely

The E-Safety Team

Appendix 4

Abbey Academies Trust
Reception & KS1 Pupil Acceptable Use Expectations
Keeping safe: Zip it, Flag it, Block it!



To help keep me safe and happy online — at school and at home.

When I use the internet, computers, iPads or any device…

1. 💻 **I only use them when an adult says it's OK.**
   I always ask before I go online or play on a device.

2. 💬 **I am kind and polite online.**
   I use kind words and never say or send anything that might hurt someone's feelings.

3. 🧠 **I think before I click.**
   I only click on links, buttons or pictures when I know they are safe.

4. 👀 **If I see something that worries or upsets me, I tell an adult straight away.**
   I don't hide it or try to fix it myself.

5. 🔐 **I keep my passwords private.**
   I can share them with my teacher or my family, but not my friends.

6. 🏠 **I keep my personal information secret.**
   I don't tell anyone my last name, address, school, or where I live.

7. 🧍 **I keep my body private online.**
   I never change clothes or show my body in front of a camera.

8. ❤️‍🩹 **I look after my friends online.**
   If I see someone being unkind, or if a friend is upset, I tell an adult who can help.

9. 😉 **I know people online might not be who they say they are.**
   I don't talk to strangers or people I don't know in real life.

10. 🎉 **I don't keep secrets about things that happen online.**
    Surprises are OK, but I always tell an adult if someone asks me to keep something secret online.

11. 📸 **I always check before sharing.**
    I don't share pictures, videos or stories of myself or others without asking an adult first.

12. 🌈 **I have fun and learn safely.**
    I use the internet to help me learn new things and be creative!

My promise:

I will follow these rules to keep myself and others safe online.

If something goes wrong or I'm not sure, I will **STOP, THINK and TELL** an adult I trust.

Appendix 5

Abbey Academies Trust

KS2 Pupil Acceptable Use Expectations

Keeping safe: Zip it, Flag it, Block it!

These rules will keep everyone safe and help us to be fair to others.



Pupil Expectations

- ✓ I have read and I understand our Abbey Academies Online Safety code.
- ✓ I will use devices and the Internet in a responsible way at all times.
- ✓ I know that Internet access may well be monitored.
- ✓ I know who to speak to if I have any concerns or problems linked to Online Safety.

To keep me safe whenever I use the internet…

1. **I ask permission first** – I will only use computers, iPads, tablets, phones, apps, sites or games when an adult knows and says it's OK.
2. **I think before I click** – I won't click on links, pop-ups or downloads unless I'm sure they're safe or an adult has said yes.
3. **I use the internet for learning and fun** – I use school logins, apps and sites for schoolwork and homework.
4. **I behave kindly online** – I treat people online the same way I would face to face. I will always use kind and polite words in messages, comments and posts.
5. **I don't share personal information** – I will keep my name, address, school, phone number, and passwords private.
6. **I keep passwords secret** – I will not use anyone else's login or password, and I'll tell a trusted adult if someone finds out mine.
7. **I know not everything online is true** – I will check with my teacher or a trusted adult if I'm not sure what I've read or seen is real.
8. **I respect age limits** – I understand some apps, sites and games are not suitable for me yet. (Most social media is 13+).
9. **I am careful with photos and videos** – I will not take or share photos or videos of anyone without their permission. I will not create or share unkind or fake pictures or videos.
10. **I keep my body private** – I never get changed or show what's under my clothes when using a device with a camera or share pictures or videos of myself or others without permission from a trusted adult.
11. **I stay safe with people online** – I only chat or play with people I already know in real life or who my trusted adults know about. I never arrange to meet anyone I've only met online.

12. **I don't pretend to be someone else online** – I will always be myself and use my real first name.
13. **I tell an adult if I'm worried or upset** – If I see something that makes me feel uncomfortable, scared, or confused, I won't hide it – I'll tell a trusted adult at home or at school straight away.
14. **I know it's not my fault if something goes wrong** – I won't get in trouble for telling the truth about something I've seen or done online.
15. **I respect other people's work** – I will not copy or use other people's pictures, words or ideas without permission. I will only edit or delete my own work.

When using ICT equipment in school …

- I know my behaviour is monitored – I understand that my use of school devices and the internet is checked to help keep everyone safe and if I am acting inappropriately then my parents/carers will be informed.
- I look after equipment – I will use school devices carefully and sensibly.
- I only play games if I have permission.
- I only access my own work – I will not look at, change, or delete other people's work.
- I use Seesaw and other school apps responsibly – My comments and uploads will always be kind, polite and about learning.
- If I make a mistake, I ask for help – I won't try to hide what I've done.
- I will not take, copy or send photographs or videos of anyone.

Appendix 6

Abbey Academies Trust
Parents/Carers E-Safety Home/School Expectations

Pupil name: _____ Class: _____

Parent/carer name: _____

E-Safety expectations:

1. **Use of technology in school**
   - I understand that Abbey Academies Trust uses digital technology as part of everyday learning, communication, and organisation, and to prepare pupils for safe and responsible use of technology in the future.
   - As the parent or carer of the above pupil, I grant my permission for my child to have access to use of the Internet and other ICT facilities at school.

---

2. **Keeping children safe**
   - I understand that the school takes **every reasonable precaution** to keep pupils safe and to prevent them from accessing inappropriate material. This includes web filtering, monitoring systems, supervision, and regular teaching about online safety.
   - I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

---

3. **Monitoring and behaviour**
   - I understand that my child's online activity on school devices and networks may be **monitored and logged** to keep everyone safe.
   - I understand that if the school has concerns about my child's online behaviour or safety, I will be informed.
   - I will support the school's rules and behaviour expectations regarding safe and sensible use of technology, including mobile phones, tablets, smart watches or similar devices.

---

4. **Supporting online safety at home**
   - I will encourage my child to follow the same safe and respectful rules at home as they do at school.
   - I will make use of parental controls, child-safe search tools and family settings where possible.

- I understand that **school networks are much safer than home networks**, so I will take steps to keep our home devices and internet safe.
- I will talk regularly with my child about their online activities, apps and games, and refer to the school website for practical advice and support.
- I understand that the school is part of 'National Online Safety' and I can access training for myself at home to keep me up to date with online issues and help keep my child safe.

---

5. Positive digital role modelling

- I will **model positive online behaviour** myself, including:
    - not posting negative or disrespectful comments about the school, staff, pupils or other parents;
    - not sharing photos or videos of children (other than my own) online;
    - following the school's policy on taking photos or videos at school events.

---

6. Social media and age restrictions

- I understand that most social media platforms (e.g. TikTok, Instagram, Snapchat, X, Facebook) are for **children aged 13 and above**.
- I will not encourage or allow my child to create accounts on platforms where they are under the minimum age.
- I will support the school's ***'Parental Use of Social Networking and Internet Sites'*** policy.

---

7. Working together

- I understand that online safety is a **shared responsibility** between school and home.
- I will talk to my child about the expectations set out in their **Pupil Acceptable Use Expectations** and help them follow these at home.
- I will contact the school (e.g. the class teacher, E-Safety Lead, or Designated Safeguarding Lead) if I have concerns about my child's online safety or the use of technology by others.

---

8. *A* positive online community

- I understand that my actions online can affect the school community.
- I will support the school's efforts to create a kind, respectful and safe online environment for all children and families.