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. **Safeguarding and Preventing Radicalisation**
8. **Use of the Internet and ICT by AAT staff**
9. **Responding to Online Safety Concerns**
10. **Data protection**
11. **Use of Ai**
12. **Courses for all school staff**

Appendix 1 – E-Safety Log

Appendix 2- Types of incidents Guidance

Appendix 3- Letters to parents/carers including pupil and parent/carer agreements

1. Rationale

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Children and young people have access to technology, and greater access to the internet, from a young age.

The purpose of this policy is to safeguard and protect all members of Abbey Academies Trust online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The policy is applicable to all members of Abbey Academies Trust. This includes staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of Abbey Academies Trust digital technology systems, both internally and externally.

School staff and governors play a vital role in setting an example for the whole school and are central to implementing policy and process. It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that schools are providing the best online safety provision they possibly can.

Our primary focus is that we teach children to keep themselves safe in the modern world.

Our school values and ethos are embedded in our 3 Rs. We:

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

This is embodied in our mission statement:

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

Abbey Academies Trust asserts that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.

Abbey Academies Trust believes that the internet and associated devices are an integral part of everyday life.

Abbey Academies Trust affirms that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

Links to other policies and statutory guidance:

- Safeguarding policy and child protection policy and procedures
- Behaviour and bullying policy
- ICT Safeguarding
- ICT Acceptable Use Within the Academy Community Policy
- Race Equality and Dealing with Racial Incidents
- Social, Moral Spiritual and Cultural Development Policy
- Staff Handbooks
- *PREVENT Duty Guidance*,
- *Keeping Children Safe in Education,*
- Anti-Extremism and Anti-Radicalisation Policy
- Code of conduct
- RSE Policy 2020
- Teaching online safety in school

- Computing, PSHE, E-Safety Curriculum Statements
- Education for a Connected World Framework
- Cyber Security Policy

2. Context and Background

The technologies:
ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices. Types of online risk usually fall under one of three categories:

Contact: Contact from someone online who may wish to bully, abuse or exploit the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting personal information.

Content: Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

Conduct: The child may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

Commerce: Risks such as inappropriate advertising, phishing and pop-up advertisements.

Current and emerging Internet and online technologies used in the academy and, more importantly in many cases, used outside of the academy by children include:

- The Internet
- Web based voice and video calling (e.g. Zoom)
- Online discussion forums
- Social networking sites (e.g. Facebook, Instagram, Snapchat)
- Messaging services (e.g. WhatsApp, Facebook Messenger)
- Blogs and Micro-blogs (e.g. X)
- Podcasting (radio / audio broadcasts downloaded to computer, tablet or phone)
- Video broadcasting sites (e.g. YouTube and TikTok)
- Music and video downloading (e.g. Apple Music, Spotify, Amazon Music)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access
- Online gaming including the use of consoles
- Photograph-sharing media (e.g. Snapchat)
- Apps on tablets and smartphones
- Use of smart speakers
- Watching Video on Demand (VOD)

Our whole academy approach to the safe use of ICT
Creating a safe ICT learning environment is based on three key elements at this academy:

• Effective hardware and software, appropriate to task;
• Policies and procedures, with clear roles and responsibilities and children made aware;
• E-Safety teaching is embedded into the academy curriculum and schemes of work

Statutory Requirements

- National Curriculum England: computing programmes of study states that children in KS1 will learn to use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies. In KS2, use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

- The Relationships Education, Relationships and Sex Education (RSE) and Health Education document states that lessons should ensure the key building blocks of healthy, respectful relationships, focusing on family and friendships, in all contexts, including online are being taught.

  During **relationships education** learning children should know:
  • that for most people the internet is an integral part of life and has many benefits.
  • that people sometimes behave differently online, including by pretending to be someone they are not.
  • that the same principles apply to online relationships as to face-to face relationships, including the importance of respect for others online including when we are anonymous.
  • the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
  • how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
  • how information and data is shared and used online.

  During **physical health and mental wellbeing** learning children should know about internet safety and harms such as:
  • about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
  • how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
  • why social media, some computer games and online gaming, for example, are age restricted.
  • that the internet can also be a negative place where online abuse, exploitation, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
  • how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
  • where and how to report concerns and get support with issues online.

  All of the bullet points above relate to 'at the end of Key Stage 2'.

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.
- 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.

Commented [LL1]: Have removed reference to Annex A

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) with pupils at the start of each school year.

Pupils

Read, understand, sign and adhere to the pupil acceptable use policy.

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 and sign the parents/carers E-Safety home/school agreement.
- Read through the pupil acceptable use agreement 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 Curriculum for pupils

6. E-Safety Curriculum

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that. At our school we are committed to teaching pupils to use ICT effectively and appropriately in all aspects of their education.

Use of the Internet by pupils
Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. **Pupils are always actively supervised by an adult** when using the internet, iPads and computers with internet access. History cannot be deleted therefore any prior browsing can be monitored.

Access for all pupils
In line with our inclusion policies across the school, we want to ensure that all our pupils have access to the internet, particularly where this will directly support their learning. If remote learning is necessary for an extended period of time, we ensure that as far as possible children are provided with appropriate resources to complete their learning. We provide access and support for pupils at lunchtimes, during before and after school clubs.

Using the Internet for learning
The internet is an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the internet for learning is part of the Computing Curriculum.
We teach all of our pupils how to find appropriate information on the internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate internet-based information as part of the Computing curriculum, and in all other curriculum areas.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.
- Children can upload their learning to an app named 'Seesaw', which is a student-driven digital portfolio that empowers students to independently document what they are learning at school.
- Parents/carers are provided with weekly guides and termly newsletters which explain how to apply safety controls at home.

Teaching safe use of the internet and ICT

Our e-safety curriculum is based on the 'Education for a Connected World' document, which is a framework to equip children and young people for digital life. As children grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and others' online behaviour. In addition, they should develop effective

strategies for staying safe and making a positive contribution online. This framework describes the skills and understanding that children and young people should have when developing understanding of online safety at different ages and key stages. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it safely.

The UKCCIS 'Education for a Connected World' framework aims to equip children and young people for digital life. It covers:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

Children should be educated in an age-appropriate way around:

- How to evaluate what they see online
- How to recognise techniques for persuasion
- Their online behaviour
- How to identify online risks
- How and when to seek support

We think it is crucial to teach pupils how to use the internet safely, both at school and at home. Abbey Academies Trust will help pupils by:

- Helping them to identify who trusted adults are.
- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations, such as Childline.
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.
- Using 'Zip it, Flag it, Block it', which encourages children to keep safe online by keeping personal information private, blocking messages and reporting inappropriate online behaviour. This digital code aims to be the 'green cross code' for internet safety.

National Online Safety

In June 2020 we joined National Online Safety (NOS). NOS is an independent online safety training provider which is run by The National College. Their mission is to educate and empower trusted adults with the information they need to engage in meaningful dialogue between children and young people about the online world, their online activities and the ever-evolving risks that they are exposed to. They focus on both general online safety risks and platform specific risks to provide adults with easy to follow information which enables conversations between adults and children.

NOS provides online CPD for parents/carers, staff and governors which the E-Safety team can track and keep a record of who has completed training. Specific training relating to E-Safety is also available for Designated and Deputy Safeguarding leads and SENCOs. This training is provided annually.

NOS also provides us with monthly webinars on trending topics to help keep staff up to date with online issues. We also receive weekly parental guides (Wake Up Wednesday) which we

upload onto the school websites and social media platforms to help keep parents/carers up to date with online platforms, devices, apps and websites their child may be using.

NOS responds to the current DfE statutory guidance around online safety including the revised 'Keeping Children Safe in Education'. We are provided with lessons and activities for EYFS, KS1 and KS2 which links to 'Education for a Connected World'.

Involvement of pupils
Pupils take an active role in their own and their peers' learning of online safety. Each class has an 'E-Safety Champion' who helps to promote E-Safety for their peers by attending meetings with the E-Safety team and participating in Collective Worships. They wear badges to show the importance of their role within the wider school community. This role supports the positive awareness of E-safety within our school and shows that the subject of online safety does not need to be daunting and should be an area that needs to be discussed.

Suitable material
We encourage pupils to see the internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching. Children only use safe methods of searching, using internet browsers.

Non-Education materials
We believe it is better to support children in finding their way around the internet with guidance and positive role modelling rather than restrict internet use to strict curriculum-based research. As well as internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-academy-hours provision, and at home. There is a selection of links to such resources available on the academy website.

Unsuitable material

Despite the best efforts of the Local Authority and school staff, occasionally pupils may come across something on the internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:
1. Making a note of the website and any other websites linked to it.
2. Informing ARK/designated safeguard lead/SLT.
3. Logging the incident – E-Safety Log (Appendix 1).
4. Discussion with the pupil about the incident, and how to avoid similar experiences in the future.

Social networking sites, chat and discussion
These forms of electronic communication are used more and more by pupils out of school and can also contribute to learning across a range of curriculum areas. We are also acutely aware of the impact of COVID 19 linked 'lockdowns' upon the amount of time pupils have spent on digital devices. We have and will continue to offer weekly 'Wake up Wednesday' posts to Facebook for each school's parents and carers to feel empowered to support their children in the latest technological developments, whether that be the latest apps, games or form of social media. We have also delivered regular E-Safety lessons via Seesaw during school closures to support pupils in a range of E-Safety themes and topics across all year groups whilst they were at home.

Social networking sites, online chat rooms and discussion forums present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

The E-Safety Champions support discussions about the safe use of social networking sites.

Pupils can upload content to their class journal on 'SeeSaw'. All content uploaded, is checked by a teacher before being posted. Only children with photo permission may have their content uploaded from a staff member to a public area of their class portal. Teachers can post content ensuring that photos and content is only seen by each specific child and their Parents/Carers.

Other online technologies (mobile phones and handheld devices)
More young people have access to sophisticated new internet-enabled devices such as smartphones, tablets and music players.

It is important that, whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc. and how the data protection and privacy laws apply.

- In general, pupils are not allowed to have personal mobile phones or other similar devices in the academy. In Years 5 and 6, children are allowed to bring a mobile to school if they need them on their journey to and from school. These are switched off and kept by the teacher during the school day.
- Any child attending Kids' Club is not allowed to use any mobile device.

Cyber Bullying - Online bullying and harassment
Cyber bullying is the sending or posting of harmful or cruel text or images using the internet or other digital communication devices.

Examples of cyber bullying which distinguishes it from other forms of bullying include:

- **FLAMING**: Cyber bullying insults can get angrier and more vulgar. The indirect and often anonymous nature of it makes the bully more likely to escalate what they say and threaten.
- **HARASSMENT**: The ease of communications results in anonymous taunts, insults, and threats which are ongoing and frequent in nature.
- **DENIGRATION**: This is the action of unfairly criticizing someone.
- **IMPERSONATION**: This is the stealing of passwords to send threatening messages including breaking into an e-mail account and sending vicious or embarrassing material to others pretending it is from someone else.
- **OUTING**: This is the sending of intimate personal information to others, for example taking a picture of a person in the locker room on a mobile device and sending that picture to others.
- **EXCLUSION**: This is ex-communication of an individual from "buddy lists" which leads to real cruelty as the person affected feels isolated and excluded.
- **CYBER STALKING**: This is blackmail (from photos) and sending of harmful messages.
- **CYBER THREATS**: Direct or actual threats to hurt or commit suicide.
- **MOBBING**: A group or gang of people that target individuals.
- **GROOMING**: Enticing or goading someone online for example to self-harm or commit a crime.

Our academy has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:

- Children are encouraged to switch the computer monitor/screen off or close the cover of the iPad when they come into contact with inappropriate or harmful content so it can be actioned appropriately.
- No access to public chat-rooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.
- Mobile devices are turned off and handed to their class teacher soon as they enter the school and are only returned at the end of the school day.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.
Complaints of Cyber Bullying are dealt with in accordance with our Behaviour and Bullying Policy.
Complaints related to child protection are dealt with in accordance with school child protection procedures.

Contact details and privacy
As specified elsewhere in this policy, pupils' personal details, identifying information, images or other sensitive details will never be used for any public internet-based activity unless written permission has been obtained from a parent or legal guardian. Pupils are taught that sharing this information with others can be dangerous – see teaching the Safe Use of the Internet.

Academy and pupil websites – pictures and pupil input
As part of Computing and the wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Deliberate misuse of the internet facilities
All pupils have discussed the rules for using the internet safely and appropriately. An E-Safety code is to be displayed in each classroom and shared areas. Where a pupil is found to be using the internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:
Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc.)

- Initial warning from class teacher
- Banning from out of school hours internet facilities (e.g. Kids' Club use of internet)
- Report to Head of School/Head Teacher/CEO/Executive Head
- Letter to parent/carer
- Removal of access to devices
- Meeting with an appropriate member of staff

Offensive material (e.g. pornographic images, racist, sexist or hate website or images etc.)

- Incident logged and reported to Head of School/Head Teacher/CEO/Executive Head
- Initial letter to parent/carer

- Removal of internet access
- Meeting with Parent/Carer to re-sign internet use agreement
- Subsequent incidents will be treated very seriously by the Head of School, and may result in exclusion and/or police involvement.

How will complaints regarding E-Safety be handled?
It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

With the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an academy computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- All incidents will be recorded in the E-Safety Log and relevant staff informed
- Interview/counselling by class teacher, Senior Leadership Team, E-Safety Coordinator, Designated Safeguarding Lead and Head of School
- Informing parents or carers
- Removal of internet or computer access for a period
- Referral to LA / Police.

Our E-Safety Leaders act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head of School/Head Teacher and CEO/Executive Headteacher.

7. 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. ~~by turning off their screen off if they see something they do not like so the matter can be addressed and logged in the E-Safety logs.~~

Commented [LL2]: I would take this line out as I'm sure it must be elsewhere.

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

The Internet
Our school understands that the internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other academies, and to engage in debate and discussion. We are committed to encouraging and supporting our school staff to make the best use of the internet and all the opportunities it offers to enhance our teaching and support learning.

Internet Availability
To enable staff to make full use of these important resources, the internet is available in the school to all staff for professional use.

ICT Equipment and Resources
The school offers staff access to appropriate ICT equipment and resources, including computers, laptops, iPads, interactive whiteboards, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software.

Professional use
Staff are expected to model appropriate ICT and internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and internet use by our pupils both in school and at home. Staff are also careful to consider inclusion and equalities issues when using ICT and the internet, and to provide pupils with appropriate models to support the academy Inclusion and Equal Opportunities policies. Staff who need support or INSET in using ICT as part of their professional practice can ask for support from the Computing Team.

Email
We recognise that email is a useful and efficient professional communication tool. To facilitate this, staff members will be given an academy email address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this email address means that they are representing the school, and all communications must reflect this.

Email accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, bulletin boards and forums, online chat and messaging
We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin boards to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

Social Networking

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in the **Policy and Agreement for ICT Safeguarding (including Social Networking) within the Academy Community.**

9. 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*.

10. 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.

11. 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 Data Protection Policy in regards to the use of Ai.

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.

12. Courses for all school staff

As part of the National Online Safety membership, there is access to an annual online safety course. Upon completion, staff gain a certificate.

Different Courses:

- **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** – 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

These courses are updated annually and are in line with current DfE 'Keeping Children Safe in Education' guidance and includes information regarding remote learning.

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

Commented [LL3]: Have added this one in.

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.

Commented [LL4]: Have added this in

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, sign one copy and return to school the attached E-Safety home/school agreement. Additionally, we ask that you read through the Acceptable Use Agreement (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 and the children will be

asked to sign the agreement. 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

Mrs Sarah Moore
Executive Headteacher

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



E 	I will be careful when going on the Internet at school, at home and if I am doing home learning.
S 	I will only use the Internet with an adult's permission.
A 	I will only click on icons and links when I know they are safe.
F 	I will be polite and kind when talking to people or writing online.
E	If I see something that worries me, I will always tell an adult.
	





I will keep my password secret, but I can tell my family and teachers. My password should be easy to remember, but hard to guess.

Your name: _____ **Class:** _____

Signature: _____ **Date:** _____

Class teacher's signature:_____

Abbey Academies Trust

KS2 Pupil Acceptable Use Agreement

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

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

Pupil Agreement

- ✓ I have read and I understand our Abbey Academies E-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 E-Safety.



To keep me safe whenever I use the internet…

- I will ask permission before using any devices (e.g. computers, iPad, tablets, mobile phones etc.) and an adult will always know when I am using equipment.
- At all times, I will think before I click and remember Zip it, Flag it, Block it when using the internet, social networks and digital devices.
- I will keep my logins and passwords private, but understand I can share them with my teachers and parents.
- I will not use another person's password and logins.
- If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it but I will immediately tell an adult in school or at home.
- When communicating online (in blogs, email, comments etc.) I will think about the words that I use and will not use words that may offend or upset other people.
- I will keep all my personal information private: name, address, school etc.
- I am aware that some websites and social networks have age restrictions and I should respect this. *(Most social networks age recommendation is 13 years old or older)*
- When posting online (e.g. on Seesaw) the comments I write, or information and work I upload, will always be polite and sensible. This includes being at school or completing home learning.
- I will not open an attachment, or download a file, unless I have permission or I know and

trust the person who has sent it.
- I understand that people online might not be who they say they are. I will not arrange to meet someone I have only been in touch with online.

When using ICT equipment in school …
- I understand that my behaviour will be monitored and if I am acting inappropriately then my parents/carers will be informed.
- I will not play games unless I have permission.
- I will only edit or delete my own files/work on the iPads and I will not look at other people's files without their permission.
- I will not take, copy or send photographs or videos of anyone.

Your name: _____ Class: _____

Signature: _____ Date: _____

Class teacher's signature:_____



Abbey Academies Trust
Parents/Carers E-Safety home/school Agreement

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

Pupil name: _____ Class: _____

Parent/carer name: _____

E-Safety agreement:
- ✓ 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.
- ✓ I know that my child has signed an E-Safety agreement and that they have a copy of the 'Acceptable Use Agreement'.
- ✓ 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.
- ✓ 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.
- ✓ I understand that the school can check my child's use of digital devices and the Internet including the sites they visit, and that if they have concerns about their E-Safety or E-Behaviour that they will contact me.

- ✓ I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's E-Safety.
- ✓ I will not take and then share online, photographs or videos of my child or other children (or staff) at school events.
- ✓ **Social networking and media sites:** I understand that the school has a clear policy on *'Parental Use of Social Networking and Internet Sites.'*
- ✓ I understand that the school takes inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

Parent/carer signature: _____

Date: _____

Executive Headteacher signature: 