Abbey Academies Trust

Every Child Matters

POLICY

For

E-Safety

Amended

New policy November 2015	**Updated January 2019**	
Updated September 2016	**Updated September 2020**	
Updated January 2018	**Updated September 2021**	

Every Child Matters within a loving and caring Christian environment

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.

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

"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

Contents of E-Safety Policy:

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 three 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 whilst caring for all in a loving 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

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 or abuse the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting person 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.

Current and emerging Internet and online technologies used in the academy and, more importantly in many cases, used outside of 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. Twitter)
- 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 includes three main 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, 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**

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Executive Head, with the support of Governors/trustees, aims to embed safe practices into the culture of the academy.

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

Leadership team
SLT's role for online safety in a school should include, but is not limited to:

- Ensure that the policy is implemented across the academy via the usual academy monitoring procedures.
- Ensure that the school has appropriate filters and monitoring systems in place.
- Upholding online safety as a safeguarding issue which is embedded across the whole school culture.

- Ensuring that children are provided with a safe environment in which to learn and develop.
- Ensuring the school has effective policies and training in place.
- Ensuring there are robust reporting channels.
- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.

E-Safety Leaders
With respect to online safety, it is the responsibility of the E-Safety Leaders to:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly.
- Develop the E-Safety Curriculum
- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Ensure that all staff are aware of procedures to follow in recognising, responding and reporting online safety concerns.
- Promote online safety and the adoption of a whole school approach.
- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.
- Collaborate with the senior leadership team and the DSL.
- Provide up to date online safety training at least annually or more in line with legislative and statutory changes and/or online safety incidents arising.
- Ensure provision of resources, support and advice to parents/carers and staff.

Governors/Trustees
The academy Governing body is responsible for overseeing and reviewing all school policies, including the E-Safety Policy.

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

With respect to online safety, it is the responsibility of the DSL to:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly.
- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.
- Collaborate with the senior leadership team, the E-Safety Leads and computing leads.
- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

School Staff

All members of school staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school; headteacher, teachers, work-experience staff, office staff, caretakers, cleaners, etc. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:

- Be responsible for promoting and supporting safe behaviours in their classrooms and for following academy E-Safety procedures.
- Be aware of and adhere to all policies in school which support online safety and safeguarding.

- Model good practice when using technology.
- Know the process for making referrals and reporting concerns.
- Know how to recognise, respond and report signs of online abuse and harm.
- Receive appropriate child protection training.
- Always act in the best interests of the child.
- Be responsible for their own continuing professional development in online safety.
- Attend training to ensure they have up to date knowledge of the curriculum and the teaching of E-Safety and refer to it regularly.
- Sign the ICT Safeguarding (including Social Networking) agreement annually.

Class teachers should ensure that pupils are aware of the E-Safety code (Appendix 5), introducing them at the beginning of each new school year.

Pupils

With respect to online safety, children need to:

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the E-Safety Code which covers their responsibilities when using ICT at school, linking to the class charter, the 3 Rs and the UNICEF Rights
- Respect the feelings of others, both off and online.
- Take responsibility for keeping themselves and others safe online.
- Know where and how to find help with any online incidents or concerns.
- Know how, when and where to report concerns and when to seek help from a trusted adult.

Each class has an E-Safety Champion, who helps to plan and deliver Collective Worships, lessons and competitions. This supports their understanding and builds confidence in dealing with E-Safety and its issues, both at home and school.

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 or abuse.
- 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. Technical and hardware guidance

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) within the Academy Community Document
- 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. 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

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 the 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. During COVID-19 lockdown and isolation periods children are provided with iPads to complete their home learning where needed. We provide access and support for pupils at lunchtimes and during before and after school out of school care.

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 now a part of the Computing Curriculum (Sept 2014)
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 taught, through E-Safety workshops and online training, 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 other's 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. 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 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 plan and deliver lessons linked to online safety. They attend meetings with the E-Safety team and take part in Collective Worships and run competitions within their Key Stage. 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 doesn't need to be daunting and should be an area that needs 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 from 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 – Minor incident E-Safety Log (Appendix 1) or Major incident E-Safety Log (Appendix 2).
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 SMART mobile phones, 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 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 (covert photos) for example taking a picture of a person in the locker room using a digital phone camera 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

Our school 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 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, pupil's 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
- 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
- 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 Executive Headteacher.

6. <u>Preventing Radicalisation</u>

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.

Our PSHE and RE provision is embedded across the curriculum, and underpins the ethos of the school. Children learn about other faiths and visit places of worship throughout the academic year. Throughout the curriculum and in particularly ICT they 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. 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 filter and to turn their screen off if they see something they do not like so the matter can be addressed and logged in the E-Safety log on the G-drive.

7. 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, data projectors, 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 ICT Team.

E-mail
We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given an academy e-mail 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 e-mail address means that they are representing the school, and all communications must reflect this.

E-mail 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 board 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.**

8. 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 or abuse 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 3 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 in both the minor and major incident logs (more guidance is provided in Appendix 3).

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,

9. Data Protection

The school has 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.

10. 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. (67 minutes)
- **SENDCOs** – Annual Advanced Certificate in Online Safety for SENDCOs (101 minutes)
- **Computing/E-Safety Leaders** – Annual Advanced Certificate in Online Safety for ICT Leads (102 minutes)
- **Safeguarding Team** – Annual Advanced Certificate in Online Safety for DSLs and Deputy DSLs (113 minutes)
- **Wellbeing Officers** – Annual Certificate in Online Safety for Mental Health Leads (78 minutes)
- **Governors** – Annual Certificate in Online Safety for School Governors (59 minutes)
- **Non – Teaching Staff** – Annual Certificate in Online Safety for Non -Teaching Staff (45 minutes)

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

11. Safeguarding and remote education during coronavirus (COVID-19)

Safeguarding teachers and pupils online

Keeping teachers safe when providing remote education is essential. Remote education is a new experience for both pupils and staff, so it's important that staff are provided support for how to approach safeguarding protection online. Online education/remote learning follows the same principles as set out in the school's code of conduct and SLT and the school's ICT support team, including ARK will offer advice, training and support in the event home learning is required. In the event of home learning, staff will be required to provide online teaching videos which will be pre-recorded for their pupils. They will engage with feedback regarding pupils' work responding professionally and adhering to the Trust's Code of Conduct. To ensure staff have support with online learning, the school will monitor these home learning resources and exchanges with pupils which are provided by teachers using Seesaw and Tapestry's admin tools. These will enable senior leaders to ensure the quality of teaching, learning as well as safeguarding procedures are adhered to at all times.

Reporting concerns

It is essential to have and communicate clear reporting routines so that children, teachers, parents and carers can raise any safeguarding concerns. Staff will continue to follow school policy for reporting any safeguarding concerns.

Each school's website and Facebook pages have been sending out/sharing useful information regarding how to report concerns online and parents/carers and children. These include signposting to useful websites, using the information on the school websites that were already there and posting weekly guides to inform parents about new devices/apps such as TikTok, how to use Zoom/Microsoft teams etc.

School staff know and use the usual route for reporting any safeguarding or online safety concerns during any school or class bubble closures.

<u>Communicating with parents, carers and pupils</u>

Where education may take place remotely, it's important for staff to maintain professional practice as much as possible.

Schools should:

- communicate within school hours as much as possible
- communicate through the school's channels approved by the senior leadership team
- use Trust email accounts (not personal ones)
- use school devices over personal devices where possible
- advise teachers do not share personal information

Recording of teaching videos

Teachers should try to find a quiet or private room or area to talk to pupils, parents or carers. When broadcasting a lesson or making a recording, consider what will be in the background for pupils to see.

Teachers will not live stream lessons.

SEND

Schools within the AAT will continue to work closely with parents/carers to provide specific resources for pupils with SEND as appropriate

Personal data and GDPR

Abbey Academies Trust continue to follow the guidance outlined in the <u>data protection: toolkit for schools</u> when managing personal data.

The senior leadership have taken into consideration that:

- contact details are not shared when e-mailing multiple people
- it is important to be careful when sharing usernames and other personal data for access to online resources
- providing access to school data systems safely

For more information regarding safeguarding and remote learning please find it here: https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

Appendix 1   *Found in policy*

E-Safety Log (Minor incidents)

<p align="center">**Abbey Academies Trust**
E-Safety Incident Log</p>

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/time of incident	Type of incident	Name of pupils/staff involved	System details	Incident details	Resulting actions and taken by whom (and signed)
09 Jan 2021 9.50 am	*A child playing a game which is certificated beyond their age.*	*Pupil:_____ Staff (Class Teacher) _____*		A child told their class teacher they were playing Grand Theft Auto at home.	Class teacher spoke to E-Safety leaders as no safeguarding concerns. Class teacher rang parents and discussed the age appropriateness of the game being played. E-Safety Leaders provided class teacher with Grand Theft Auto Wake Up Wednesday Guide for Parents.

Appendix 2

School Incident E-Safety Log (Major incidents)

<u>**Abbey Academies Trust**</u>

<u>**Incident Log**</u>

Name of Parent/s involved:

Name of Child: **Class:**

Date of Incident: **Time of Incident:**

People Present:

Log completed by:

Please check the box that best describes what happened. Please choose all that apply.

☐   An inappropriate website is accessed <u>**unintentionally**</u> in school by a teacher or a child.

☐   An inappropriate website is accessed <u>**intentionally**</u> by a child.

☐   An inappropriate website is accessed <u>**intentionally**</u> by a staff member.

☐   An adult or child uses schools ICT equipment inappropriately.

☐   Bringing inappropriate electronic files from home.

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

☐   Teasing, name calling, making critical remarks or threatening in person, by phone, by e-mail, etc.

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

☐   Using other people's logins and passwords maliciously.

☐   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

- ☐   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

- ☐   Cyber bullying (bullying by calling, texting, emailing, web posting, etc.)

- ☐   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.

- ☐   Other

If you select other, please describe:

Background to the incident:

Log Content: which should include action/s agreed and any further meeting dates necessary:

Signed as a true record of events by all staff members involved

Signed: *Date:*

Print name(s)

<u>Appendix 3</u>

<u>Types of incidents with guidance on what to do</u>

An inappropriate website is accessed <u>unintentionally</u> 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 <u>intentionally</u> 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 <u>intentionally</u> 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.

<u>**Appendix 3 cont.**</u>

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 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 a major 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 4
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!

ZIP IT — Keep your personal stuff private and think about what you say and do online.

FLAG IT — Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

BLOCK IT — Block people who send nasty messages and don't open unknown links and attachments.

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.
T		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.
Y		I won't tell anyone any personal details such as where I live or my last name.

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:_____

ZIP IT — Keep your personal stuff private and think about what you say and do online.

FLAG IT — Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

BLOCK IT — Block people who send nasty messages and don't open unknown links and attachments.

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: