



Abbey Multi Academy Trust Policies & Procedures

Online Safety Policy

Approved on

1 September 2026

Approved by

Abbey MAT Board of Trustees

Next review due

30 September 2027

Contents

1. Introduction and Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety.....	10
5. Educating parents about online safety	11
6. Cyber-bullying	12
7. Acceptable use of the internet in school	15
8. Pupils using mobile devices in school.....	15
9. Staff using work devices outside school	15
10. How the school will respond to issues of misuse	16
11. IT Systems	16
12. Using the Internet and Email	17
13. Publishing content online	18
14. Training	19
15. Monitoring arrangements	20
16. Links with other policies	21
Appendix 1: KS2, KS3, KS4 and KS5 acceptable use agreement (pupils and parents/carers)	1
Appendix 2: EYFS and KS1 acceptable use agreement (pupils and parents/carers).....	2
Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors).....	3
Appendix 4: online safety training needs – self audit for staff.....	4
Appendix 5: online safety incident report log.....	5
Appendix 6: Filtering and Monitoring	6

1. Introduction and Aims

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies staff, children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Making /receiving phone calls via their mobile phones
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

This online safety policy recognises the commitment of our school to online safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The online safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

Abbey Multi Academy Trust aims to ensure its academies:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content means being exposed to illegal, inappropriate or harmful content. This may include pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation, conspiracy theories, harmful AI-generated content, manipulated images, deepfakes and content generated or altered by artificial intelligence.

Contact means being subjected to harmful online interaction. This may involve other users, adults posing as children or young adults for the purpose of grooming or exploitation, commercial

advertising, peer-to-peer pressure or generative AI applications that simulate human interaction in a way that may expose children to risk.

Conduct means online behaviour that increases the likelihood of harm or causes harm. This includes online bullying, abusive or misogynistic messages, making, sending or receiving nudes and semi-nudes, sharing explicit images, AI-generated intimate imagery, deepfakes, deep nudes, impersonation and the use of technology to harass, coerce or humiliate others.

Commerce means risks such as online gambling, inappropriate advertising, phishing, financial scams, fraud, exploitation through online platforms and risks linked to persuasive or manipulative digital design.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

This policy should be read alongside the Trust's Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Data Protection Policy, Digital Device Policy and any academy-specific procedures relating to mobile phones, filtering and monitoring.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Trust board and governing bodies will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor or trustee with oversight of safeguarding will include online safety, filtering and monitoring within their safeguarding oversight. Each academy will also identify the senior leader responsible for filtering and monitoring locally.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Read, understand, contribute to and help promote the school's online safety policies and guidance as part of the school's overarching Safeguarding procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement their online safety strategy
- Ensure the school has filtering and monitoring arrangements in place.
- Monitor the school's implementation of filtering and monitoring systems
- Review data derived from the monitoring system and quality assure the actions taken when alerts are received.

- Liaise with the senior leadership team, DSL and IT service provider to review provision annually.
- Seek assurance that the filtering and monitoring standards for schools are being met.

The Trust Board, local governing bodies and academy leaders will ensure that the effectiveness of filtering and monitoring arrangements is reviewed at least once every academic year. This review will be led by the named senior leader responsible for filtering and monitoring, with the support of the Designated Safeguarding Lead and IT support. The review will include checks that filtering and monitoring systems are working effectively across all relevant school-owned devices, networks, user groups and locations where pupils access the internet through school systems. A written record of the review, checks undertaken, issues identified and actions completed will be retained for safeguarding assurance.

3.2 The Headteacher / Principal / Head of School

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The headteacher will:

- Ensure liaison with the Governors
- Develop and promote an online safety culture within the school community
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required

3.3 The Senior Leadership Team

The Senior Leadership Team are responsible for:

- Documenting decisions on what is blocked or allowed and why
- Reviewing the effectiveness of filtering and monitoring provision
- Overseeing reports

The SLT are responsible for making sure that all staff:

- understand their role and responsibilities in relation to online safety, including filtering and monitoring
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns
- work closely with governors and trustees, the designated safeguarding lead (DSL) and the IT service providers in all aspects of filtering and monitoring

Each academy will identify a named senior leader with responsibility for filtering and monitoring. This senior leader will ensure that filtering and monitoring arrangements are understood, reviewed, checked and acted upon. They will work with the DSL and IT support to ensure that systems remain effective, that concerns are escalated promptly and that records are maintained for safeguarding and governance assurance.

3.4 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school anti-bullying policy
- Updating and delivering staff training on online safety, including filtering and monitoring (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Work closely with the IT service provider to ensure that the filtering and monitoring system meets the needs of the academy

The DSL will oversee and act on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

This list is not intended to be exhaustive.

The DSL will understand the filtering and monitoring systems and processes in place at the academy, including how concerns are identified, reported, escalated and reviewed. The DSL will work with the named senior leader for filtering and monitoring and IT support to ensure that safeguarding concerns arising from filtering or monitoring alerts are responded to promptly and recorded appropriately. This responsibility will be reflected in DSL role descriptions and safeguarding training arrangements.

3.5 The ICT manager / IT Technical Staff / IT Service Provider

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material (see appendix 6 for details)
- Procuring filtering and monitoring systems for all Trust academies

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on an ongoing basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and malicious attack
- Report any online safety related issues that come to their attention
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the school's ICT equipment.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

The IT technical staff / service provide will have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT technical staff / service provider will work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

- Working with the DSL to ensure that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy Read, understand and help promote the school's online safety policies and guidance
- Taking responsibility for ensuring the safety of sensitive school data and information
- Developing and maintaining an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintaining a professional level of conduct in their personal use of technology at all times
- Ensuring that all digital communication with pupils is on a professional level and only through school-based systems, NEVER through personal email, text, mobile phone social network or other online medium.
- Embedding online safety messages in learning activities where appropriate
- Supervising pupils carefully when engaged in learning activities involving technology
- Ensuring that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Reporting all online safety incidents which occur in the appropriate log and/or to their line manager
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Undertake training on online safety including filtering and monitoring
- Follow policies, processes and procedures in relation to filtering and monitoring
- Act on reports and concerns about online safety including those linked to filtering and monitoring

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Help and support the school in promoting online safety

Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology

Consult with the school if they have any concerns about their child's use of technology

support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - [UK Safer Internet Centre](#)

Hot topics - [Childnet International](#)

Parent factsheet - [Childnet International](#)

[Healthy relationships – Disrespect Nobody](#)

3.8 Students

We expect students to:

- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings of other students
- Ensure they respect the rights of other students
- Ensure they respect the values of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow school policies regarding bullying
- Students will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

3.9 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

Primary schools:

In **Key Stage 1**, pupils will be taught 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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Secondary schools:

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

All schools:

Pupils will also be taught, in an age-appropriate way, about generative AI, AI-generated content, deepfakes, impersonation, misinformation, manipulated images, online coercion and the importance of reporting any content or interaction that makes them feel unsafe, uncomfortable, pressured or targeted.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

The Trust will support parents and carers to understand emerging online risks, including AI-generated content, deepfakes, harmful online interaction, mobile phone use, filtering and monitoring arrangements and routes for reporting concerns.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they

can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their class/tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from [S.Collier / D.Murfin / J.Binks]
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to [the staff member in conjunction with the DSL (D.Murfin) / headteacher (S.Collier) / other member of staff (J.Binks)] to decide on a suitable

response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI), deepfakes and AI-generated content

Generative artificial intelligence tools, including text, image, audio, video and chatbot systems, are increasingly accessible to pupils and adults. These tools may offer educational benefits but they also create safeguarding, ethical, data protection and behaviour risks.

Abbey Multi Academy Trust recognises that AI may be used to create, alter or circulate harmful content, including misinformation, impersonation, deepfakes, AI-generated images, AI-generated audio or video, nudification content, deep nudes and nudes or semi-nudes generated or altered using AI. The Trust also recognises that some generative AI applications may simulate human interaction in ways that could expose pupils to harmful content, unhealthy relationships, grooming-type behaviours or coercive interaction.

Any use of AI to manipulate, harass, impersonate, deceive, bully, coerce or humiliate another person will be treated seriously and managed in line with the Trust's safeguarding, behaviour and anti-bullying arrangements. Where AI-generated content includes, appears to include or is alleged to include nude or semi-nude imagery of a child, staff must not view, copy, forward or share the image. The concern must be reported immediately to the DSL who will follow the Trust's safeguarding procedures, UKCIS guidance and any required referral routes.

Staff must complete an appropriate AI impact and safeguarding risk assessment before introducing new AI tools into learning, administration or pastoral systems. This must consider pupil access,

filtering and monitoring, data protection, age appropriateness, transparency, human oversight and the potential for misuse.

Pupils will be taught to recognise, question and report AI-generated or manipulated content. Staff will receive training so they understand AI-enabled safeguarding risks, including deepfakes, nudification apps, impersonation, simulated interaction, harmful content generation and AI-facilitated child-on-child abuse.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, trustees and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, trustees, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Abbey Multi Academy Trust expects academies to operate as mobile phone-free environments for pupils during the school day, unless an individual plan confirms an agreed exception. This means pupils should not access or use mobile phones or personal devices during the school day, including lessons, tutor time, movement between lessons, breaktimes, lunchtimes, clubs or activities organised by the academy unless explicitly permitted by a member of staff for a specific educational, medical, safeguarding or accessibility reason.

Where a pupil requires access to a device for medical, SEND, safeguarding or other agreed reasons, this must be documented through the appropriate individual plan and managed by the academy. Any misuse of a mobile phone or personal device will be managed in line with the academy behaviour policy, safeguarding procedures and acceptable use expectations.

Refer to the Trust's Mobile and Smart Technology policy for details regarding mobile phone use in schools.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

The Trust ensures that all laptops provided for use inside and outside school have

- Anti-virus and anti-spyware software installed
- Up-to-date operating systems with the latest updates installed

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from a member of IT support.

If you are provided an iPad the Trust, you will be required to read and sign a Digital Device Policy which contains further details specific to that device.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use – adapt according to what policies you have. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. IT Systems

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information.

Cyber security is recognised as part of the Trust's safeguarding arrangements because compromised systems, inappropriate access, loss of personal data or disruption to safeguarding records may create risks to children. Academies will maintain appropriate cyber security controls, access management, account management, password protections, backup arrangements, malware protection and incident response processes. Any cyber incident that may affect pupil safety, safeguarding information, personal data or the availability of key safeguarding systems must be reported promptly in line with the Trust's safeguarding, data protection and IT incident procedures.

11.1 Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).
- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.
- All pupils have a unique, individually-named user account and password for access to IT equipment and information systems available within school.
- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains a log of all accesses by users and of their activities while using the system in order to track any eSafety incidents.
- Password must be difficult to guess and should be a mixture of upper case and lowercase, numbers and symbols. strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Students will have to reset their passwords at given intervals.

12 Using the Internet and Email

12.1 Internet

We provide the internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

12.2 Using Email

Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

All email activity is recorded in line with data protection laws. The school is able to view these records in situations where this is called upon.

It is the personal responsibility of the email account holder to keep their password secure.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

School will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils.

Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses.

Responsible use of personal web mail accounts on school systems is permitted for staff only outside teaching hours.

12.3 Receiving Emails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source

13 Publishing content online

13.1 School Website:

The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number.

Identities of pupils are protected at all times. Parents have the option to opt out so that photographs of individual pupils are not published on the website. Group photographs do not have a name list attached.

13.2 Online Material Published Outside the School:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Further information can be found in the Safe Working Practice Guidance

13.3 Using Images, Video and Sound

We recognize that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

The academy recognises that images published online may be copied, manipulated, altered or misused, including through artificial intelligence technologies. Before publishing images, the academy will consider whether publication is necessary and proportionate and will take reasonable steps to minimise risks to children.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress.

In line with GDPR regulations, we will ask all parents/carers to give permission for their child to be photographed or videoed (in publications and on websites) when they start at the academy and at periodic intervals. Parents / carers will be able to opt-out at any time should they wish to do so.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events, except in specific circumstances where rights holders refuse permission, but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites and can be only used for their personal use.

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

Training will also include awareness of how artificial intelligence can be used for grooming, misinformation, image manipulation and the creation of harmful or misleading content.

Staff will also receive training on:

- AI-generated content, including deepfakes, deep nudes and manipulated imagery
- AI-enabled harassment, bullying and impersonation
- Nudification applications and AI-generated nudes and semi-nudes
- Harmful interactions through AI chatbots and other generative AI systems that simulate human interaction
- The safeguarding implications of AI-generated content and how concerns should be reported
- Their responsibilities in relation to filtering and monitoring systems, including how to recognise, escalate and respond to concerns

Staff will be reminded that concerns involving AI-generated or digitally altered sexualised images of children must be treated as safeguarding concerns and reported immediately to the Designated Safeguarding Lead.

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. This training will include understanding the academy's filtering and monitoring systems and processes, how alerts are reviewed and escalated, how online safeguarding concerns are managed, and the implications of emerging technologies including artificial intelligence.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. Advice on how to log issues related to online safety can be found in appendix 5.

This policy will be reviewed every year by the CEO. At every review, the policy will be shared with the trust board and governing body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

16. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

Digital Device Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: KS2, KS3, KS4 and KS5 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the way pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	
Are you aware of how the filtering and monitoring systems in place at your academy?	
What are your responsibilities in relation to filtering and monitoring?	
Are you aware of the Trust's approach to AI use and associated risks? Do you know what actions to take if you suspect a pupil has used or been targeted by AI-generated content (e.g. deepfakes)?	

Appendix 5: Logging online safety incidents

All online safety incidents and concerns should be recorded promptly, accurately and factually in the academy's safeguarding recording system.

The purpose of recording is to:

- enable effective safeguarding decision-making
- provide a clear chronology of events
- identify patterns of behaviour or emerging risks
- support risk assessment and intervention
- provide evidence of action taken
- support referrals to external agencies where necessary

Staff should record what they have seen, heard or been told and distinguish clearly between fact, opinion and professional judgement.

Online Safety Recording Checklist

When recording an online safety concern, staff should consider whether the following information has been included.

Basic Information

- ☐ Date of concern
- ☐ Time concern occurred (if known)
- ☐ Date reported
- ☐ Name of pupil(s) involved
- ☐ Year group and tutor/class
- ☐ Name of member of staff making the record
- ☐ Location where concern was identified
- ☐ Whether incident occurred:
 - ☐ In school
 - ☐ At home
 - ☐ In the community
 - ☐ Unknown

Nature of the Concern

Which category best describes the concern?

- ☐ Harmful content
- ☐ Harmful contact
- ☐ Harmful conduct
- ☐ Online commerce or exploitation
- ☐ Cyberbullying
- ☐ Child-on-child abuse
- ☐ Sexual harassment
- ☐ Sharing of nudes or semi-nudes
- ☐ Online grooming
- ☐ Extremism or radicalisation
- ☐ Self-harm or suicide content
- ☐ AI-generated content or deepfake imagery
- ☐ Online fraud or financial exploitation
- ☐ Data protection or privacy concern
- ☐ Filtering and monitoring concern
- ☐ Other

Record What Happened

Has the record included:

- ☐ What was observed?
- ☐ What was disclosed by the child?
- ☐ Who disclosed the concern?
- ☐ When did it happen?
- ☐ How did staff become aware?

- ☐ Exact words used where appropriate?
- ☐ Details recorded factually and objectively?
- ☐ Any screenshots, URLs or evidence secured in accordance with school procedures?

Technology Involved

If known, record:

- ☐ Device involved
- ☐ School-owned device
- ☐ Personal mobile phone
- ☐ Tablet
- ☐ Laptop
- ☐ Gaming device
- ☐ Other

Platform or service involved:

- ☐ Social media
- ☐ Messaging app
- ☐ Email
- ☐ Gaming platform
- ☐ AI tool/chatbot
- ☐ Website
- ☐ Video platform
- ☐ Unknown
- ☐ Other

Immediate Safeguarding Considerations

Consider whether the record addresses:

- ☐ Risk of harm to the pupil

- ☐ Risk of harm to other pupils
- ☐ Emotional wellbeing impact
- ☐ Bullying or harassment
- ☐ Sexual abuse concerns
- ☐ Child-on-child abuse concerns
- ☐ Exploitation concerns
- ☐ Risk of self-harm
- ☐ Risk of suicide
- ☐ Criminal behaviour
- ☐ Vulnerable pupils involved
- ☐ SEND considerations
- ☐ Wider safeguarding concerns identified

Artificial Intelligence (AI) Considerations

Where relevant, has the record identified whether the concern involved:

- ☐ AI-generated imagery
- ☐ Deepfake content
- ☐ AI-generated nude or semi-nude imagery
- ☐ AI-enabled cyberbullying
- ☐ AI impersonation
- ☐ AI manipulation or misinformation
- ☐ AI chatbot interaction
- ☐ Other AI-related concern

Actions Taken

Has the record clearly stated:

- ☐ Immediate action taken
- ☐ Who was informed
- ☐ DSL notified
- ☐ Headteacher informed (where required)
- ☐ Parent/carers informed (where appropriate)
- ☐ Device secured
- ☐ Evidence preserved
- ☐ Filtering or monitoring review undertaken
- ☐ Risk assessment completed
- ☐ Referral made to external agency

External Agency Involvement

Where relevant:

- ☐ Children's Social Care
- ☐ Police
- ☐ Prevent
- ☐ LADO
- ☐ CAMHS
- ☐ Early Help
- ☐ Internet Watch Foundation
- ☐ CEOP
- ☐ Other agency

Review and Follow-up

The record should clearly identify:

- ☐ Next actions

- ☐ Responsible person
- ☐ Timescale
- ☐ Review date
- ☐ Need for ongoing monitoring
- ☐ Need for curriculum or wider safeguarding response
- ☐ Need to review filtering and monitoring arrangements

Appendix 6 – Filtering and Monitoring

Filtering Designed For Schools

The Schools Broadband online filtering and Safeguarding Incident Management Service, supports schools in both their DfE and KCSiE filtering and monitoring compliance, as well as providing an enhanced aid to Safeguarding Leads in their management of children and young people's online activity.

Filtering billions of categorised URLs, our filter provides education-specific safe searches across all popular web search engines including Google, Bing and YouTube, in over 40 languages; this is one of the most advanced education specific filters available.

Safeguarding Incident Management For Schools

As an enhancement to our service, the Safeguarding Incident Management Platform supports schools in integrating the management of digital pupil behaviour with off-line pastoral concerns as part of a wider coordinated approach to safeguarding. This further supports schools' KCSiE and Prevent Duty compliance.

Providing instant real-time alerts on keyword searches and visited sites of interest, the platform enables school staff to identify concerns and trends, share information and intervene immediately where required. Please see our separate product sheet on the Safeguarding Incident Management Platform.



The Schools Broadband Advantage

Filtering both image and text-based content we protect over 700,000 children and young people in UK schools, giving schools the ability to tailor filtering policies to suit their own school environments. This can be as simple or sophisticated as you need it to be.

A combination of shared URL and IP address lists from our customers' most used sites and services, together with machine learning, means our filtered categories are automatically updated, filtering new safeguarding threats as soon as they emerge.

Strengthened Protection

To further strengthen the protection we provide, we work closely with the following government agencies:

Counter Terrorism Internet Referral Unit (CTIRU)

National Crime Agency (NCA)

National Cyber Security Centre (NCSC)

We provide pupil level filtering at network level as default, ensuring safeguarding always remains intact.



Regulatory Compliance

Our filtering service supports full compliance with the following requirements:

Prevent Duty

Keeping Children Safe in Education

Internet Watch Foundation (IWF) Block List and Image Hash List

Home Office Terrorism Block List

UK Safer Internet Centre



Proactively Manage Online Safeguarding

Monitor signs of online bullying, Prevent Duty risks and safeguarding threats with automated alerts and reporting.

Dynamic, out of the box reports can be emailed to your Designated Safeguarding Leads for daily management and easy, swift investigation of safeguarding issues.

Comprehensive, up to date incident reports as well as historic reports (up to two years) and browsing data going back 6 months is also available to aid safeguarding investigations.

For security, all monitoring and reporting information is only accessible remotely when signed in safely behind your firewall or onsite on your own school network.

Predefined report templates can be scheduled by DSLs, enabling pupil intervention at an early stage if required.

Reports highlight blocked searches and sites, enabling identification of individual, class, form, or school-wide blocked events. Also highlight repetitious attempts to reach inappropriate content.

Proactive alerts to Designated Safeguarding Leads can be created from day one, providing key information on searches and site data, enabling timely information for potential interventions.

