# POLICY

For

# ICT Safeguarding (including Social Networking) within the Academy Trust Community

| | | |
|---|---|---|
| **September 2017** | **September 2020** | **September 2023** |
| **September 2018** | **September 2021** | **September 2024** |
| **September 2019** | **September 2022** | **September 2025** |

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

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

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

*John Wesley*

As a RRS (Rights Respecting School – UNICEF) this upholds the following articles from the UNCRC (United Nations Convention on the Rights of the Child):

Article 3: The best interests of the child must be a top priority in all actions concerning children.
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 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 36: Every child has the right to be protected from doing things that could harm them.

Our Abbey Academies Trust (AAT) policy for ICT Safeguarding is based upon the premise that all life is from God and we are created in the image of God. Pupils' personal, social, health and emotional development are all promoted in the supportive Christian ethos of the school, where all are respected, valued and encouraged. The Trustees, Governors and staff take seriously their responsibility to safeguard and promote the welfare of the children and young people in their care.

AAT provides the use of cameras, computers, laptops, electronic handheld devices and internet facilities, for children and staff. The cameras, including those on iPods, iPads and tablets, allow staff and pupils to record activities going on in the school. Technology provides opportunities to enhance education by supporting with learning activities, providing information for the planning of activities and for communication both internally and externally with fellow professionals and families, while also promoting digital literacy and safe, responsible use.

New technologies are integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- there are set guidelines and rules on the use of school ICT resources for staff and volunteers
- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems, Trust/school reputation and/or users at risk
- that staff are protected from potential risk in their use of technology, including cyber and information security, in their everyday work

The Trust will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users of this technology and equipment.

This policy should be read and used alongside the E-Safety Policy, AAT Cyber Security Policy and Child Protection and Safeguarding Policy.

*The bullet points below are not an exhaustive list. The school reserves the right to amend this list at any time. The AAT leadership team and/or governing body/trustees will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.*

***The ICT system is owned by AAT and has appropriate software to ensure safe internet use. The Trust reserves the right to examine or delete any files that may be held on its system or to monitor any internet sites visited.***

**Devices**

- School laptops and iPads remain the property of the AAT at all times and as such should not be used for personal use nor should they be personalised with stickers etc
- Damage or faults involving equipment or software should be reported immediately
- No hardware or software should be installed without reference to the Chief Operating Officer and ARK ICT
- All computers MUST be locked if left unattended
- All laptops should be stored out of sight, or preferably locked away, when the school is closed
- System security must be adhered to and no password provided by the Academy Trust or other related authority must be disclosed
- Passwords should be changed regularly
- Personal data i.e. information about individuals, must be kept secure and used or accessed appropriately, whether in school, taken off the school premises or accessed remotely
- School staff should not use memory sticks/portable drives to store personal or sensitive information. If this is unavoidable, for whatever reason, these devices must be encrypted and data deleted as soon as possible
- Some key information is stored on external drives as backups. These files are stored securely within school
- Multi-factor authentication is used to reduce the change of unauthorised access to personal/trust data

**Internet Use/Activity**

- Activity that is found to be unsuitable or that attacks or corrupts other systems or infrastructure is forbidden
- Accessing or attempting to access any sites that contain any of the following: child abuse or exploitation; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive, including information of an extremist nature, is prohibited
- The use of Trust devices for gambling is forbidden
- Staff will immediately report any illegal, inappropriate or harmful material or incident, including accidental access to or receipt of inappropriate materials, or filtering breach they become aware of, to a Leader or a member of the Senior Leadership Team
- Staff must not use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials
- The school's ICT facilities should not be used to bully or harass someone else or to promote unlawful discrimination
- Staff members' online activity, both in and outside school, must not bring the school, their professional reputation, or that of others, into disrepute
- Copyright of materials must be respected
- Other users' files will not be accessed without their permission
- The Academy Trust's email, internet and any related technologies must only be used for professional purposes or for uses deemed 'reasonable' by the CEO/Executive Head Teacher, Heads of School, Board of Trustees or Local Governing Body

**Photographs**

- Children should use iPads to take photographs and record videos for learning purposes. Any photographs or videos not required for further use should be downloaded or deleted periodically
- Staff must only use the school's own digital cameras or electronic handheld devices to take any photographs or videos and these, if not required for further educational use, must be deleted periodically
- Photographs, videos and any media involving children from the school, must not be taken or stored on any devices other than those provided by the Academy Trust
- Images should only be taken and used in line with our Academy Trust policy and the wishes of parents/carers, and must not be distributed outside the Academy Trust network without authority

**Emails** (*Please see AAT Cyber Security Policy for additional email guidance)*

- E-mail correspondence and messages sent must be responsible and uphold professional standards
- Hyperlinks or attachments to emails should not be opened unless the source is known and trusted, or if there are concerns about the validity of the email. If a member of staff is in any doubt of the validity or source of an email, they should contact ARK ICT before opening said email (see Cyber Security policy for further information)
- Users are responsible for all e-mails sent and for contacts made that may result in emails being received
- Users are responsible for ensuring that emails are not sent to the wrong email address by mistake
- Any unusual or suspicious emails or messages must be reported immediately to the SLT and ARK ICT
- Staff must take extra care when sending sensitive or confidential information by email. Any emails being sent outside AAT that contain sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. This is done by prefacing the subject box with 'EncryptMail, space, subject title
- Only the approved, secure email system (Outlook) should be used by employees for Academy Trust business.
- If outside agencies (e.g. Lincolnshire Music Service, Inspire+ etc…) require email access or printing capabilities, they will be provided with a school email and user account if appropriate
- Personal details such as mobile numbers and email addresses must not be given to pupils and or parents/carers
- Emails MUST not be displayed on the class board/screen and should be kept out of sight of others, special care should be taken when opening confidential emails

**OneDrive**

- The Trust's OneDrive should be used for work purposes only
- Do not store personal files on the Trust OneDrive
- Ensure that any folders that are shared are shared carefully with correct addresses checked before sharing
- Only share files with specific individuals, never with "everyone" or the "public".
- Be careful sending links to shared folders because they can often be forwarded to others who you did not provide access to
- Remember that once a file is shared with someone and they download it to their device, they can share it with others
- Remove individuals when they no longer require access to files or folders
- Wherever possible, the OneDrive should be accessed using your school device. If you are using a non-school device to access the OneDrive, it must be secure and only accessible through a password or appropriate authentication. You should not share these details with anyone else. Always report any accidental sharing, data loss or suspected breach immediately to the Data Protection Officer.

**Pupils**

- **Pupil use of electronic devices must be supervised at all times**
- School will work with parents/carers to ensure they are aware of internet use
- Pupils will use only age-appropriate software in the school
- Any inappropriate access to materials by pupils must be reported to a member of the Senior Leadership Team
- The internet sites visited will be monitored. On iPads this will be done via the iPads search history which cannot be erased on each iPad. 2 members of the safeguarding of the safeguarding team in each school also receive a weekly 'Securly' report, detailing lists of sites which were blocked upon attempt to access. Any concerns or patterns will be reported appropriately
- We will display the rules for safe internet use throughout the school
- Any pupils who need to bring a mobile phone to school will store these with teachers for the whole day, including time at Breakfast Club and/or Kids' Club. They will not have access to this during the school day and should only use these off-site at the start or end of the school day
- Pupils are not permitted to bring tablet computers or internet enabled games consoles to school at any time. This includes to Breakfast Club and Kids' Club
- 'Smart watches' which allow access to photographs and other similarly restricted content on mobile phones are not to be used by pupils in school
- Pupils will not be permitted to take mobile phones on day or residential visits

**Mobile phones – staff**

- Staff may not use their personal mobile phone whilst working in school or in lessons
- Mobile phones should always be kept out of sight, even when switched off during the school day
- School's telephone number should be given out to be used as an emergency contact for staff
- Staff may use their mobile phones during breaks, which are taken in the staff room or an appropriate area separate from all pupil contact and view
- Staff may not use any camera facility on their personal devices (phones, watches etc…) within school hours or on educational visits
- Images of pupils/staff must never be taken or stored on personal devices which includes (but is not limited to): mobile devices; laptops; internal camera memory; memory sticks or portable hard drives

**Social Networking Sites** *(The school has guidelines for staff on appropriate security settings for Facebook accounts - see appendix 1)*

- Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times
- Staff should at no time post anything regarding children, their parents/families or other staff at our school
- No reference should be made in social media to pupils, parents/carers or school/academy staff
- Staff should not engage in online discussion on personal matters relating to members of the school community which may bring the school/academy into disrepute
- Personal opinions should not be attributed to the school/academy or Trust
- Social Networking Sites should not be accessed via work computers or during the school day for <u>personal</u> use
- Staff must be aware at all times of the need to keep personal and professional lives separate and maintain professionalism whilst using social networking sites
- Staff should not accept friend requests from a person believed to be a parent, a pupil or a recent ex-pupil except in circumstances where a member of staff has ongoing personal contact with a parent outside of school
- No photographs from the school may be used, or ones which identify the school or children from the school on personal social media accounts
- No photographs of other members of staff to be used without their consent

- Anyone posting remarks which breach confidentiality or are deemed to be of a detrimental nature to the Academy or other employees may be subject to disciplinary proceedings
- Any employee, who becomes aware of social networking activity that would be deemed distasteful or not appropriate, should make a leader or a member of the Senior Leadership Team aware
- The personal use of social media must neither interfere with a member of staff's ability to maintain their professional reputation nor impact on the reputation of the school
- School social media sites are to be administered by **at least** two members of staff
- Any incidents involving social media may be dealt with under school/academy disciplinary procedures

**School social media accounts**

- All schools within the Trust have an official Facebook page and YouTube page, managed by members of the computing and/or leadership team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account

**Filtering and Monitoring**

Abbey Academies Trust use an industry-standard filtering system, Securly, as recommended by ARK ICT to block access to inappropriate content, as per government recommendations. In addition, the filtering system will be regularly reviewed and updated to ensure it remains effective at blocking harmful content. The software uses filtering to help monitor the appropriate use of staff and pupil use of the internet. Please read this policy in line with AAT's E-Safety Policy, AAT's Cyber Security Policy and the Filtering and Monitoring Action Plan.

Only designated staff, such as the DSL, CEO / Executive Headteacher and ICT Technicians, will have the authority to override filtering restrictions, and this will be done only for legitimate educational purposes. In addition, the IT service provider will have technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports to the Executive Headteacher / DSL
- Completing actions following concerns or checks to systems.

Each school as an assigned filtering and monitoring governor to challenge and ask questions about our policies and practices.

Equally, it is important to understand that no filtering system can be 100% effective. This is why monitoring of internet usage (both staff and pupils) as of particular importance. Abbey Academies Trust will use monitoring to track internet usage and identify any potential safeguarding concerns. Unlike filtering, monitoring does not stop users from accessing material through internet searches or software. The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited/attempted to visit
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications
- Only authorised staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law

**The school monitors ICT use in order to:**

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation

- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation
- Comply with KCSIE requirements

It is the teaching staff's responsibility to monitor pupils' online behaviour during lessons and report any concerning activities to the DSL. All staff will be vigilant in ensuring that during any online use, pupil activity is monitored. It is recognised that this monitoring strategy is required to minimise safeguarding risks and may include:

- Physical monitoring by staff watching the screens of users
- Network monitoring using logs files of internet traffic and web access
- Individual device monitoring through the use of third-party software.

Pupils will be educated about the school's monitoring practices, emphasising the importance of responsible internet use. This is done through a variety of ways, including specific activities on National E-Safety Day, the election of pupil E-Safety Warriors who then promote this message in Collective Worships and a dedicated E-Safety lesson as part of Computing lessons every month.

Our filtering system, Securly, provides alerts to the DSL and Head of School when the filtering system has been attempted to be breached. After an attempted breach the DSL/Head of School, or another member of the safeguarding team, will investigate the alert and take appropriate action in line with the Trust's E-Safety Policy and Safeguarding Policy. Alerts and actions taken are logged and regularly reviewed by the DSL.

If a child has been found to be using ICT inappropriately, action will be taken in line with AAT's E-Safety Policy and AAT's Behaviour and Bullying Policy.

If a member of staff has been found to be using ICT inappropriately, breaching AAT's Staff Code of Conduct and E-Safety Policy, action will be taken in line with AAT's Disciplinary Policy.

Policy Reviewed: September 2025
Next Review: September 2026

Appendix 1: Facebook sheet for staff

**Don't accept friend requests from pupils on social media**

**School staff on Facebook**

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

---

**Check your privacy settings**

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

**You're being harassed on social media, or somebody is spreading something offensive about you**

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

**Abbey Academies Trust ICT Safeguarding Policy for Staff and Other Adults within the School Community (e.g. Trustees, Governors, PTFA, Parent Helpers, Volunteers, Pupils)**

**Please sign and return this page only and retain your copy of the policy:**

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.
I understand that if I fail to adhere to this Acceptable Use Policy Agreement, I could be subject to disciplinary procedures and my contract may be terminated.

I agree to follow the ICT Safeguarding Policy and to support the safe and secure use of ICT throughout the School:

Signature ……..

Date ……..

Full Name ……
(printed)

Job Title …….