Abbey Academies Trust

Every Child Matters

POLICY and AGREEMENT

For

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

Amended

September 2016	**September 2019**	
September 2017	**September 2020**	
September 2018	**September 2021**	

Every Child Matters within a loving and caring Christian environment

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 as 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 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 and tablets, allow staff and pupils to record activities going on in the school. Technology provides opportunities to enhance education by helping with learning activities, providing information for the planning of activities and for communication both internally and externally with fellow professionals and families.

New technologies have become 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:

- 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 and 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 school 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.

Acceptable Use Policy Agreement

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 students / 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.

Photographs

- Children should use the child friendly digital cameras, iPods or 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.

Computer and internet use

The computer 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.

- School laptops 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.
- Activity that is found to be unsuitable or that attacks or corrupts other systems is forbidden.
- Accessing or attempting to access any sites that contain any of the following: child abuse; 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. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL. 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.
- Staff members online activity, both in and outside school, will not bring the school, their professional reputation, or that of others, into disrepute
- 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.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- Only the approved, secure email system should be used by employees for Academy Trust business.
- If outside agencies (e.g. Lincolnshire Music Service, Premier Sport etc…) require email access or printing capabilities, they will be provided with a school email and user account.
- E-mail correspondence and messages sent must be professional and responsible.
- Personal data i.e. information about individuals, must be kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Executive Head Teacher, Head Teacher, Heads of School, Board of Trustees or Local Governing Board. Personal or sensitive details taken off site electronically, must be encrypted.
- No hardware or software should be installed without reference to the Executive Administrator.
- Use for gambling is forbidden.
- Copyright of materials must be respected.
- All computers should be locked if left unattended.
- Data should regularly and securely be backed up.

- All laptops should be stored out of sight, or preferably locked away, when the school is closed.
- Hyperlinks or attachments to emails should not be opened unless the sources is known and trusted, or if there are concerns about the validity of the email. If a member of staff is any doubt of the validity or source of the email they should contact ARK before opening any email.
- Any unusual or suspicious emails or messages must be reported immediately to the SLT and ARK ICT.
- 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 details such as mobile numbers and email addresses must not be given to pupils and or parents/carers.

Rules for Responsible Internet Use

- Other user's 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 Executive Head Teacher, Head Teacher, Heads of School, Board of Trustees or Local Governing Body.
- Any form of external storage, including pen drives, USB or cloud storage will not be used without prior permission and must be encrypted.
- Internet access will only be used for agreed reasons.

Pupils

- School will work with parents/carers to ensure they are aware of internet use.
- Children will use only age-appropriate software in the school.
- All internet activity should be deemed appropriate.
- E-mail correspondence will be directed only to people who have been approved and messages sent will be polite and responsible.
- Personal details will not be shared over the internet.
- Arrangements to meet others will not be made via the internet.
- Any inappropriate materials sent 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
- We will display the rules for safe internet 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 within school hours or on educational trips.
- 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

- 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 students/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 Sties should not be accessed via work computers or during the school day for personal use. However, where appropriate, teachers and other staff members may post content to Facebook and Twitter on the school's accounts, in relation to learning and other educational experiences. They may also post links to these on the school website as long as the children in question have permission for this. Training will be provided to staff on how to create and post appropriate social media content.
- Staff must be conscious 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 personal contact with a parent outside of school (e.g. through a club).
- 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 their Leader/a member of the Senior Leadership Team aware.
- Content used for planning and learning materials must only be sent via emailed and no personal information must be stored on personal devices in relation to this.
- 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 these sites may be dealt with under school/academy disciplinary procedures

COVID 19 and home education

Since the Coronavirus (COVID 19) outbreak in 2020, schools have had to adapt to allow for education to take place at home during periods of lockdown. As a result of this, the AAT is having to adjust to remote education strategies both in the present as well as planning for potential future lockdowns. While this is happening, the school will take every precaution to ensure that teachers are safe when undertaking remote education. **When delivering online education, teachers should follow the same principles set out in the school Code Of Conduct.**

- Teaching from home is different to teaching in the classroom. Teachers should try to find a quiet area to talk to pupils/parents or carers. When pre-recording a lesson, teacher should consider what will be in the background/visible on screen
- Lessons must not be 'live-streamed', nor teachers engage in any video-calling
- Any lessons/ videos produced as part of online learning should be pre-recorded and not delivered 'live'

- Staff to ensure that, if they are delivering teaching at home where significant amount of data is being uploaded (e.g. in the form of teaching videos) that they don't incur surprising costs (e.g. mobile data access charges)
- ARK/SLT will be on hand to support with technical issues as long as their own working situation allows
- Where possible, ensure that school provided electronic devices (e.g. laptops or school iPads) are used to provide home learning resources
- Only Seesaw and Tapestry should be used to communicate and deliver lessons/activities/feedback for home learning. No additional programs or software should be used without prior consent from SLT
- Resources/videos should be provided and created on a class/group basis. Any individual resources (e.g. SEND) must be approved by SLT/SENCos
- No personal data or information should be shared via online learning
- Professional standards and expectations should be adhered to at all times
- If communicating with children/parents/carers via the messaging/chat feature, staff must ensure responses are of a high professional standard
- Any responses to parents/carers/children must be made in the hours 8am-5pm
- If a complaint or concern is raised then normal school procedures/practices apply
- Any safeguarding concerns must continue to be followed via normal school procedures

Policy Reviewed: September 2021
Next Review: September 2022

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

Staff Signature

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

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 …….