Abbey Court School Trust

Date agreed and implemented by board 4 July 2024

Review date 4 July 2027

E-SAFETY POLICY

"This policy should be read as part of a collection of policies that together form the overall Safeguarding Policy and procedure for Abbey Court School."

All staff employed at Abbey Court and Abbey Court School Trustees are subject to this policy.

This policy covers:

1. **Social Media Networking**
2. **Sexting**
3. **Sensible use of e-mail/Internet/mobile phones**

Section 1 - Social Networking

1. Introduction

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our School Community and partners, our legal responsibilities and our reputation.
For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

2. Purpose

The purpose of this policy is to ensure:

- all children are safeguarded
- that Abbey Court School, and its Trustees are not exposed to legal risks;
- that the outstanding reputation of Abbey Court School Trust, is not adversely affected;
- that any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of Abbey Court School.

3. Scope

This policy covers the use of social networking applications by School Employees and Governors and by partners or other third parties (eg Trustees) on behalf of the School.

These groups are referred to collectively as 'Staff' for the purpose of this policy.
The requirements of this policy apply to all uses of social networking applications which are used for any school or local authority related purpose regardless of whether the applications are hosted corporately or not. They must also be considered where Staff are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to:
Blogs, Online discussion forums, Collaborative spaces, Media sharing services, and 'Microblogging' applications. Examples include Twitter, Facebook, Instagram, Snapchat, WhatsApp, YouTube etc.

Many of the principles of this policy also apply to other types of online presence such as virtual platforms.

All Staff should bear in mind that information they share through social networking applications, even if they are in private spaces, is still subject to Copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School and Local Authority Equality and Safeguarding Policies.

Staff must also be aware that involvement in discussion groups, blogs and social network

systems (e.g. Facebook and Instagram) should be for personal interest only and not offer opinions, views or photos that could bring the reputation of the school into disrepute Linking on social media with a parent(s) of the school is discouraged unless these are family members. Any such link should be notified to the Headteacher/Chair of Trust

Any communication received from children to Staff must be immediately reported to the Head Teacher, Designated Safeguarding Lead and procedures for safeguarding followed.

If a School Representative is made aware of any other inappropriate communications involving any child and social networking, these must be reported immediately, using the above procedures.

The school internet policy must be used at all times when children use ICT and access the internet in school (See the Computing policy).

4. Staff Training

The policy is introduced to staff during their induction and subsequently regular opportunities are scheduled to discuss further.

5. Enforcement

Any breach of the terms set out below could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible School representative being suspended.

The Local Authority reserves the right to require the closure of any applications or removal of content published by Staff which may adversely affect the reputation of the School or put it at risk of legal action.
Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority's Dismissal and Disciplinary Policies apply.
Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

Abbey Court Community School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Section 2 'Sexting': Definition and Advice

There are several definitions but for the purposes of this advice sexting is defined as:

Images or Videos that are sexual or are indecent and are generated

- by pupils, or
- of pupils

These images are shared by young people and/or adults via a mobile phone, handheld device or website.

Steps to take in the case of an incident:

1. Follow the standard child protection and safeguarding policies.
2. Record the incident and immediately report it to the Designated Safeguarding Lead (DSL)
3. Do not search a device, copy or print out 'evidence' simply inform the DSL who will decide upon the appropriate course of action.

Section 3 - Sensible use of emails/internet/mobile phones when driving: Applies to Private Phones

This guidance applies to all email/Internet use, whether it is at school, or at home.

Computer Viruses/hacking/scam emails/texts are a constant threat, and they are always evolving to "beat the system". Computer Viruses/hacking/scam emails/texts spread in a variety of ways, but with more and more people using the Internet and emails to communicate, this is the most common medium for the distribution of viruses or to target individuals with scam emails/texts. New viruses/scam emails and texts are found every day, so all of us need to be careful when opening/reading emails, and when using the Internet in general.

Common file extensions for viruses are .doc .exe .zip .pif .scr and .com (although there are others). The email/text message itself will normally consist of a short message along the lines of "Please see the attached file" or "Hey there, how are you doing" (although this message will vary).

If this file is opened, it will 'infect' the machine, or device and the virus will do what it has been programmed to do, which is normally to restart your machine, delete files on your machine, and send copies of itself to as many other machines or devices as possible.

On a computer or mobile phone, to enable the virus to spread, it will look at your email/phone program's address book, and send an infected message to everyone you know (which is how you will often receive infected emails from someone you have regular contact with).

As a rule of thumb, it is best to delete any message that you are not sure of, especially if it has an attachment. You can often receive infected messages from people that you know, but you should be able to tell if the message is genuine or not.

When a colleague sends an email with an attachment, they will normally put your name at the start, a message in the middle, and their name at the end of the message. They would not normally just say "Look at the attachment".

If you are not sure about it, you should ask the person before you open it. If they say no – delete it!

Medway LA has virus detection software on the email system that detects *most* viruses before they even reach our inboxes, but unfortunately, it cannot block everything. Abbey Court also uses anti-virus software at IP level.

If you use your own email account at home, your email provider may have a similar system in place, but this is not always the case. Microsoft can provide useful information at windowsupdate.microsoft.com. It is also important that each machine that connects to the Internet has an up-to-date virus scanner installed. The virus scanner will alert you to any suspicious files and will help you get rid of any viruses that your computer may pick up.

Examples of commonly used anti-virus software are Norton Anti-virus, Sophos Anti-virus and McAfee Virus Scan (there are many others available from a variety of retailers).

Similarly, the same can apply to mobile phones so contact your network provider who can advise.

Summary:

- If you get any suspicious looking emails/texts – Delete them straight away.
- It should not harm your computer/mobile device if you just read an infected message. The harm is done when you open the attachment.
  Do not open any attachments you are not sure of.
- If you get a message from someone you know – try to compare it to the "usual" messages you receive from that person. If it just tells you to look at an attached document – it is probably a virus.
- Make sure you have an up-to-date virus scanner on your home machine.
- You should visit the Microsoft downloads site to ensure your home machine is always protected against known vulnerabilities in Windows and related software.
- Ensure you regularly update your phone software via your mobile phone provider. If you are unsure, contact your mobile phone provider for advice.

Monitoring and Review

This corporate policy must be communicated at both a corporate and directorate level to ensure all staff are aware of its contents. This policy will be reviewed after the first year of implementation to assess the effectiveness of the measures introduced and then on a 3-yearly basis or after a significant event whichever is the sooner.

Mobile phone cameras

For the purpose of safeguarding children and confidentiality, staff must not use their mobile phones whilst in school (including educational visits; work experience; inclusion etc.). The school provides digital cameras for this purpose. The use of a personal Mobile Phone to take photos of pupils in any context would also be a breach of confidentiality and would lead to disciplinary action.

Mobile phones can only be used in agreed areas i.e. the staff room and areas of the premises outside of the main building.

APPENDICES

Abbey Court School

Acceptable Internet Use Agreement for Staff

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Acceptable Use Agreement has been drawn up to protect users.

The school reserves the right to examine or delete any files that may be held on its computer network system or to monitor any Internet sites visited including on any portable devices owned and provided by the school for staff to use for school purposes. The Network Manager/IT Technician recall devices at least twice a year for updates and checks;

You are agreeing to the following:

- All Internet activity via the school network, should be appropriate to staff's professional activity or the student's education;
- Access should only be made via the authorised account and password, which should not be made available to any other person at any time;
- When accessing/completing work from home, you must maintain confidentiality at all times and lock your computer when you are away from it;
- Whilst it is not practical nor appropriate to restrict access to the internet by the staff at home, any school information remains confidential and must not be shared or published via the internet. This will constitute a breach of confidentiality (reference the Confidentiality Policy).
- Activity that threatens the integrity of the school computing systems, or activity that attacks or corrupts its, or other systems, is forbidden;
- The use of school computing systems for sending private e-mails is prohibited at all times and the school has the right to monitor the school systems to ensure adherence to this agreement.
- Users are responsible for ensuring compliance to this agreement for all e-mail sent and
- Where a school device is used to access personal emails, you are responsible for insuring nothing inappropriate is downloaded to the device.
- Where a personal device is used to access work emails, you are responsible for abiding by the same rules which apply to the use of a school device as outlined in this Agreement.
- As e-mails can be forwarded, intercepted or inadvertently be sent to the wrong person, the same professional use of language and content should be applied as for letters or other media used in school;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;

- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Use of the school network or a school device, to intentionally access inappropriate/unsuitable materials such as pornographic, racist, drugs or offensive material is forbidden.
- Where inadvertent access to inappropriate/unsuitable website(s) occurs, staff must report this immediately to the Network Manager/IT Technician.
- Staff must be aware that involvement in discussion groups, blogs and social network systems (e.g. Facebook and Instagram) should be for personal interest only and not offer opinion, view or photos that could bring the reputation of the school into disrepute. The discussion of issues and information pertaining to Abbey Court School, would be a breach of confidentiality and would lead to disciplinary action. Linking on social media with a parent(s) of the school is discouraged unless these are family members. Any such link should be notified to the Headteacher.

Full name:_____

Signed:_____ Date:_____