St Andrew's
BERKSHIRE

Online Safety Policy

At St Andrew's we work consistently and proactively together to promote the welfare of children and protect them from harm.

Statement of Principles
This policy aims to ensure that all pupils and staff at St Andrew's use technology in such a way as to protect and promote the welfare of all members of the community, and of the pupils in particular.
At St Andrew's we aim:

- To ensure that pupils are appropriately supervised during school activities.
- To promote responsible behaviour with regard to activities online.
- To ensure that staff and pupils have the knowledge, skills and confidence to become safe and responsible users of the Internet and other communication technologies.
- To take account of legislative guidance, in particular the General Data Protection Regulations and the Data Protection Act 2018.

Policy Reach
The policy for online safety applies to all pupils, staff, governors and volunteers working at the School who have access to, and are users of St Andrew's IT systems and resources both in and out of school. It applies to all electronic devices and services provided, whether accessed within School or at an external location.
It is designed to sit alongside, and should be read in conjunction with, other related policies and documents, such as:

- IT Acceptable Use Policies (staff and pupils/parents)
- Anti-Bullying Policy,
- Behaviour Policy
- Bring Your Own Device and Remote Working Policy
- Child Protection and Safeguarding Policy
- Device Acceptable Use Agreement (pupils)
- Device Expectations (Y7&8 pupils)
- Email Guidelines (staff)
- Social-Media Policy
- Staff Behaviour and Code of Conduct Policy

The Head Master will be responsible for the implementation of this policy and ensure that staff are aware of this guidance.

1. WHAT IS ONLINE SAFETY?

Whilst the Internet and associated technologies are excellent tools and resources to enrich learning, there are still issues related to their use. Some examples of these might include:

- Cyberbullying – typically, malicious messages or images sent via email, social media and messaging services such as WhatsApp, Snapchat or Instagram.

- Potential exposure to inappropriate and/or adult content – for example, sexual, racist or extremist.
- Sexting – sharing of explicit images or Youth Produced Sexual Images
- Illegal behaviour – including hacking, spamming or viewing/downloading pirated media/games, easy access to gambling platforms.
- Inappropriate content and titles of WhatsApp groups.
- Potential exposure to sexual predators posing as peers; this could include grooming
- Downloading malware, viruses, Trojans, trackers/loggers that are packaged anonymously within software, apps or web pop-ups.
- Using proxy or VPN services to purposely bypass the filtering services.

The School will assume responsibility for protecting all members of our community from such dangers by technical means (such as filtering and monitoring) and by educational means designed to ensure that pupils and staff understand how to operate safely online.

2. RESPONSIBILITIES:

All users are expected to model safe, responsible and professional behaviours in their own use of technology. On joining, parents of pupils below Year 6 will sign the IT Acceptable Use Policy (Pupils). Pupils in Year 6 or above will sign themselves. Pupils from Y6-8 sign a Device Acceptable Use Form annually. Staff are required to review the IT Acceptable Use Policy (Staff) as part of their induction. PLT proposes that this is issued to and signed by staff annually.

All Staff
Online safety will be the concern of all staff at St Andrew's. All adults acting in *loco parentis* and who come into contact with children have a 'duty of care' for them, and this duty of care extends to all matters relating to the use of technology. All staff who work at St Andrew's will receive regular training in their child protection responsibilities; all staff will receive specific training in matters of online safety, including use of the internet and cyberbullying.
All staff will have a clear understanding of online issues, know how to report concerns, abide by the staff AUP (Acceptable Use Policy), give due concern to the reputation of the School and its members before they post online, contribute to a whistleblowing culture where they have any suspicion or concern, and never befriend current pupils or recent leavers on social media themselves.

Other responsibilities include:
• to supervise and guide pupils carefully when engaged in learning activities involving online technology, and use common-sense strategies in learning resource areas where older pupils have more flexible access.
• to report any misuse to the Safeguarding Team in line with the reporting procedures outlined in the Safeguarding policy and KCSIE 2023.
• to take professional, reasonable precautions when working with pupils, previewing websites and resources before use; and using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Designated Safeguarding Lead (DSL)
The DSL will have an operational duty to act as the lead person in matters of Child Protection and Safeguarding. The Designated Safeguarding Lead should take lead responsibility for online safety and understanding and review of the filtering and monitoring systems and processes in place.
They will also be responsible for overseeing online safety, alongside the Head of Digital Learning, within the curriculum. They ensure that online safety incidents are logged as a safeguarding incident and that all staff are aware of the procedures that must be followed in the event of an incident as outlined in our

Child Protection and Safeguarding policy. The DSL communicates regularly with the Senior Leadership Team, Pastoral Leadership Team, St Andrew's Committee, and IT support to discuss current issues, review incident logs, adjust filtering and amend operational procedures.

Head of Digital Learning
The Head of Digital Learning is regularly updated on current online safety issues and legislation, and is aware of the potential for serious child protection concerns. They support and work with the DSL with day-to-day responsibility for online safety issues and also play a leading role in establishing and reviewing the school's online safety documents. An awareness and commitment to online safety is promoted across the School community by facilitating training and advice for all staff while ensuring online safety education is embedded within the curriculum. The Head of Digital Learning liaises with the DSL to monitor the impact of online safety training and assesses future training needs

All Pupils
All pupils at the School will contribute to the ethos of St Andrew's by showing respect for and understanding of the needs of others. In addition, they will comply with the AUP (Acceptable Use Policy) each time they login to the St Andrew's network. St Andrew's is a talking school, with a culture of openness and transparency and pupils will report any concerns they may have regarding online safety issues (see Section 7).

Parents and Carers
The School will endeavour to assist parents with their awareness of developing technologies and give advice on how to support children towards safe, responsible and appropriate use of the internet and social media. To support families in helping their children use technology safely, our school will seek to provide information and awareness to parents and carers through:
• Guidance on technology use and reference to relevant resources and websites in letters and the Weekly Messenger
• Parents' evenings
• External speakers and workshops
• High profile national events e.g. Safer Internet Day
It is recommended parents and children develop their own Online agreement to use at home that is respected and followed by all members of the family.

FILTERING AND MONITORING

A progressive filtering system (Securly) blocks sites that fall into sensitive categories (e.g. adult content, race hate, gambling) and ensures age appropriate access to resources based on educational needs. The DSL keeps a log of all changes to filtering systems. Amendments are made in consultation with the Digital Lead and IT Support. Automatic and immediate alerts are set up to flag any suspicious language used or inappropriate searches, on the internet as well as for Microsoft Teams documents and email. Should a child type anything into their laptop that is of concern, it is flagged automatically and immediately by the monitoring software and the DSL receives an email with details of the search, time and user. Any alerts that are a cause for concern will be followed up by a member of the Pastoral or Safeguarding team as appropriate. The St Andrew's network has been secured to appropriate standards suitable for educational use.
Teachers use Senso, which is a classroom management software to help maintain control, keep students focused and ensure that they are working online safely. Teachers can easily identify students who are off task and remove online distraction with real-time monitoring and restrict browsing functionality using this software.

NB -during school holidays, whilst any devices provided by the School will retain existing filtering systems put in place, they will not be monitored to the same extent that they are in termtime. This will be communicated with parents.

3. COMMUNICATION

Staff Communication
Staff are instructed to always keep professional and private communication separate. Use of email and internet for personal purposes is permitted but any such use must be limited and must not disrupt staff duties. Staff members who wish to communicate with pupils online may do so only with the approval of St Andrew's, using official St Andrew's sites and accounts created specifically for this purpose. These sites are managed and controlled by St Andrew's administrators. There should be no connection made between any personal accounts and school accounts used for educational purposes. Use of any school approved social networking will adhere to the Social Media Policy. Teachers are advised that they should use a separate email address just for social networking so that any oth er contact details are not given away. They should also be aware that they can be vulnerable to unintended misuses for electronic communication. Email, texting and social media encourage casual dialogue and often innocent actions can easily be misconstrued or manipulated. Social networking sites blur the line between work and personal lives and discretion should be used at all times with both parents and colleagues. Staff are expected to regularly review their privacy settings to ensure that profiles and photographs are not viewable to the general public. See also, Email Guidelines.

Pupil Communication
Pupils are taught about social networking, email, acceptable behaviour and protocols, and how to report misuse, intimidation or abuse through our online safety curriculum. Pupils in Y6-8 are required to sign and follow our Device Acceptable Use Agreement. Pupils in Y7 and 8 also sign and follow Device Expectations.

4. EDUCATION

The School supports and trains children in online safety through a variety of different methods:

- Across the curriculum in all subjects
- Workshops and communication on online safety training for children and parents
- Through assemblies
- Through our Digital Ambassadors (pupil-led committee)
- IT curriculum covering safe internet usage
- Through PSHE lessons
- Through the Tutor System
- Study diaries for Y5-8 have an Online Safety page with tips and recommendations for staying safe online.
- Posters with the Childline number are around the School.

5. USE OF MOBILE PHONES

The School does not permit the use of mobile phones by pupils in acknowledgement of the fact that children have "unlimited and unrestricted access to the internet" which may facilitate abuse in school.

All members of staff working in EYFS will not use or carry personal mobile phones or any other electronic device with imaging and sharing capabilities while working. Staff may use their phones during break and lunchtimes in the staffroom only. All staff working in the early years setting and with early years children must ensure that if they wear a smart watch this is either switched off or switched to

flight mode. Designated school iPads may be used to take photos and record information for Tapestry and the children's Learning Journals.

In the Prep School, personal devices should not be used when a child/children are present during lesson times. They should only be used in the presence of children in the event of an emergency or when a landline phone is not available to seek assistance.

6. INCIDENT MANAGEMENT AND REPORTING

All members of the St Andrew's community are encouraged to be vigilant and report issues, in the confidence that they will be dealt with quickly and sensitively.

Pupils
Pupils are taught to recognise when they are at risk and how to get help when they need it. They are taught what to do should they see content online they are uncomfortable with. They are also taught to block anyone or anything who contacts them that might be harmful.

The pupils are provided with different methods for reporting an incident:

- Talking to an adult
- Use the Online Safety Questions in their ICT Team
- Use an Online Bother Box in their Form Team
- Use a physical Bother Box around School
- Report online e.g. to CEOP

Staff
If any concerning content or images are found on an electronic device the device should be locked and the DSL contacted immediately. Members of staff should not view images, look for further images, copy or print any images or forward images by email or any other electronic means. Support may be sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues. The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.