St Andrew's

BERKSHIRE

E 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 e-based activities.
- To take account of legislative guidance, in particular the General Data Protection Regulations and the Data Protection Act 2018.

Policy Reach
The policy for E-Safety applies to all pupils, staff and volunteers working at the School. It also applies to members of the St Andrew's Committee. It is designed to sit alongside, and should be read in conjunction with, other related policies such as the Child Protection and Safeguarding Policy, the Anti-Bullying Policy, the Behaviour Policy, the Acceptable Use Policy, and the Social-Media
Policy. The Head Master will be responsible for the implementation of this policy and ensure that staff are aware of this guidance.

What is E-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 material.
- 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.
- 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 internet filtering) and by educational means designed to ensure that pupils and staff understand how to operate safely online.

All Staff

E-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 E-Safety, including use of the internet and cyberbullying.

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 staff will have a clear understanding of E-Safety issues, know how to report E-Safety 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.

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 E-Safety issues. All pupils will know how to report E-Safety concerns or problems by telling a trusted member of the School Staff. They can also use the virtual forms in their ICT Teams to report any concerns.

Designated Safeguarding Lead (DSL)

The DSL will have an operational duty to act as the lead person in matters of Child Protection and Safeguarding. They will also be responsible for delivering E-Safety, alongside the Head of Digital Learning, within the curriculum.

Document Review History

Last review date: January 2023	**Next review date:** January 2024

Owner: Deputy Head Pastoral