St. Andrew's School.
Policies and Procedures.

Information and Communications Technology Acceptable-Use Policy

Whilst St. Andrew's encourages the creative use of Internet, Digital and Mobile Technology for learning, we recognise that all members of staff are responsible for the safeguarding of pupils and the appropriate use of ICT resources both internally and externally.

This policy must be read in conjunction with St. Andrew's Safeguarding Policy and Staff Code of Conduct.

Also with reference to the following Education Development Trust Policies:-

- IT Access Control & Password Policy
- Clear Desk and Screen Policy

Computer Equipment

Computers, laptops, tablets and other networked resources are available to staff in the school. These resources are intended for administrative and educational purposes, and may only be used for legal activities consistent with the rules and policies of the school.

All staff must take appropriate security measures to protect laptops, tablets, and any peripheral devices (for example digital cameras).

It is expected that staff will use computers as appropriate within the curriculum and that they will provide guidance and instruction to pupils in the use of the online curriculum. The computers, laptops and tablets are provided and maintained for the benefit of all staff. If a member of staff requires a laptop outside of school they must seek permission before doing so. When offsite, staff must continue to follow the guidelines outlined in this policy.

Email and Messaging

The school e-mail account will be the principal point of contact for all electronic communication and should be used for all correspondence involving school business.

Whilst our ICT support services provide filtering and virus protection staff should not:

- Use strong language, swearing or aggressive behaviour
- Open attachments to emails unless they come from someone you already know and trust. (They could contain viruses or other programs that would destroy all the information and software on your computer)
- Send or receive emails (or other forms of digital messaging) containing material that is likely to be unsuitable for children (This applies to any material of violent, dangerous, racist, or inappropriate content). If staff have any concerns over correspondence they receive electronically they should **not** delete the message and report the incident to a member of the SLT immediately.

Social Networks

St. Andrew's understands that you may use the internet, email and other types of electronic communication (including instant messaging and social networks like Facebook and X) in your personal lives. However, many sites such as social networks have public visibility and staff must not post any content that may compromise the school safeguarding policy, staff code of conduct or post anything that may bring St. Andrew's or Education Development Trust into disrepute. The School owned IPods can be used to post appropriate news to the School Twitter and Facebook pages.

Computer Equipment
Permission must be sought before taking any IT devices off site. When using IT devices outside of school the acceptable usage policy still applies.
Teachers must not –

- Install or attempt to install, device drivers and software on the laptops without permission from the network administrator.
- Change settings on computers or laptops unless authorised by the Computing Co-ordinator, this includes Internet settings, browsers and system preferences

If using a laptop in or out of school you are continuously responsible for it. Any damage must be reported to the Computing Leader immediately.

You must not allow any external agency or support service to tamper with St. Andrew's hardware or software. Appropriate and safe care and storage of St. Andrew's laptops is expected at home.

Definitions of Unacceptable Usage
Unacceptable use of St. Andrew's computers and network resources may be summarised as, but not restricted to:

- Actions which cause physical damage to any ICT hardware, including peripherals (e.g. mouse, cables, wiring)
- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate
- Threatening, bullying, intimidating or harassing staff, students or others
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights
- Defamation
- Unsolicited advertising, often referred to as "spamming"
- Sending emails that purport to come from an individual other than the person actually sending a message using, e.g. a forged address
- Attempts to use the ICT facilities for the purposes of bribery
- Attempts to break into or damage computer systems or data held thereon
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, e.g. use of equipment which is inadequately protected against viruses and spyware
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised
- Using the school network for unauthenticated access
- Using the ICT facilities for gambling
- Using the ICT facilities for carrying out any illegal trading activity
- Any other conduct which may discredit or harm the school, its staff or the ICT Facilities

Privacy and Monitoring

Passwords

Passwords will automatically require update every 30 days – please see below password criteria.

- be kept confidential (passwords may not be shared at any time)
- consist of a minimum of 12 characters
- consist of mixed case alphabetic characters
- contain at least one number or special character (e.g. %, &, $, *)
- be suitable to commit to memory so it isn't necessary to write them down
- be temporary at issue and changed after first log-on

Staff are reminded that the user is responsible and accountable for all activities carried out under their username. It is each member of staff's responsibility to keep their own and the school's data secure.

All staff must log off or lock their pc, laptop or device when they are not at the machine, this includes short periods of time or when accessing the school's drives remotely. At the end of the day it is important staff 'shut down' their computer and, where relevant, turn off the overhead projector so updates and backups can run.

Staff **must not**

- Share their passwords with anyone else (this is excepting shared accounts such as some of the Administrative accounts where it is recognised that passwords may need to be shared).
- Have their passwords on display or store their password where it may be found by others.

The school reserves the right for appropriately authorised staff to examine any data including personal data held on school systems.

It is also occasionally necessary to intercept network traffic. In such circumstances appropriately authorised persons will take all reasonable steps to ensure the privacy of service users. Logs will be kept of usage of ICT equipment; this will include dates and times when accounts were accessed.

Once a staff member has left the school the school holds the right to refuse access to emails and data stored on its network.

Printing
Whilst St. Andrew's realises that printing is necessary we encourage all staff and pupils to print responsibly. Printing should not be for personal use. St. Andrew's monitors printing and the SLT hold the right to change print quotas at any time.

Laptops

Pupil Laptops
Networked laptops are available use in the Years 1-6. The teaching staff member is ultimately responsible for the collection, transportation and safe return of each laptop to and from the laptop trolley. Any faults must be immediately reported to the Computing Leader.

Principles – BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.
- You must not engage in activities involving social media, which might bring St. Andrew's into disrepute.
- You must not represent your personal views as those of St. Andrew's on any social medium.
- You must not discuss personal information about pupils, and other professionals you interact with as part of your job on social media.
- You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or St. Andrew's.
- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of St. Andrew's.

- You must decline 'friend requests' from pupils if you receive any on your personal social media accounts.

- You must not discuss any personal information about pupils and their family members and colleagues, or any personal web space.
- Caution is advised when inviting work colleagues to be 'friends' on personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships.
- Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking, so that any other contact details are not given away.

Mr J Pitcher
Computing Leader
St. Andrew's School

Policy Date: 1st September 2026
Review Date: September 2028