E-Safety Policy

Adopted September 2026
Review September 2027

ST ANNE'S PRIMARY SCHOOL, DENTON
E-SAFETY POLICY (2.0)

Introductory Statement
St Anne's School believes that pupils should be equipped with the right ICT skills to enable them to apply such skills as appropriate in their day to day academic work. Pupils should be able to make intelligent choices about when to use ICT as a tool across the curriculum. We will teach the pupils not only to be able to make choices about using technology, but also about how to use this technology safely, in school and at home. The skills already developed will be harnessed and applied in a more educational context in school to optimise children's learning and subsequent attainment.

Possible risks while using technology in school are

- Children might access Internet content of an unsavoury, distressing or offensive nature or receive inappropriate or distasteful emails

- Children might receive unwanted or inappropriate emails from unknown senders, or be exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites, such as Facebook or Twitter

- Chat rooms provide cover for unscrupulous individuals to groom children

However, the benefits of using the technology are

- Children are equipped with skills for the future

- The Internet provides instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available

- The Internet helps to improve children's reading and research skills

- Email, messaging and networking helps to foster and develop good social and communication skills

- Technology helps to bring the curriculum to life – 'Excellence and Enjoyment.' i.e. Children can access 'real' weather reports and data when studying locations in geography; Children can go on a 'virtual' tour of a place or museum in a history lesson.

These benefits far outweigh the risks involved so long as users in the wider school community are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

This policy, written in accordance with BECTA and Local Authority guidelines, focuses on each individual technology available in school and outlines the procedures in place to protect users in school and beyond and the sanctions imposed if these are not adhered to.

Procedures for Use of the School Network

The following procedures must be followed by all staff, children and visitors when using the school network:

- Staff, children, community and guest users must access the school network using their own log-ons and log-ons must not be shared
- Users must respect confidentiality and no attempt should be made to access another individual's personal folder on the school network without permission
- School staff are able to access the children's folders for the purposes of assessment
- Software should not be installed on the school network without prior permission from the Senior Leadership Team or ICT subject leader
- Machines must never be left 'logged on' and unattended in school unless it is only for a short time and the machine is 'locked' (use Ctrl+alt+del followed by 'lock computer')
- Machines must be 'logged off' correctly after use

Procedures for Use of the Internet, Email and VLE

- Children, staff, community and guest users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in school
- Parental or carer consent is requested on entering the school in Reception, in order for children to be allowed to use the Internet or email in school
- Users must access email using their own log-on / password and not those of another individual and passwords must remain confidential and no attempt should be made to access another user's email account
- The Internet and email must be used only for professional or educational purposes
- Children must be supervised at all times when using the Internet and email
- Procedures for safe Internet use are displayed in each classroom and all pupils are taught about e-safety
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the SLT and the IT support Teaching Assistant
- Internet and email filtering software is installed on the school network to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence and is reviewed and updated regularly

- Internet and email use will be monitored regularly in accordance with the General Data Protection Regulation (GDPR)

- School e mail addresses are not assigned to individual pupils

- Pupils must not disclose any information of a personal nature on the Internet including mobile and home phone numbers, addresses, or anything else which might allow them to be identified

- Children's communications to other schools/organisations will be sent via the teacher or another member of staff, who will then vet the content and relay any replies back to individual children once they have been approved

- All communications sent should be courteous and the formality and tone of the language used appropriate to the reader

- No strong or racist language will be tolerated and appropriate sanctions will be imposed on any users who break this code

- Bullying, harassment or abuse of any kind will not be tolerated and appropriate sanctions will be imposed on any users who break this code

- If users are bullied, or offensive communications are received, this must be reported immediately
  (Children should tell a teacher in the first instance. All other users should report this to a member of the SLT. Communications received should not be deleted but kept for investigative purposes)

- Anti-virus software is used and regularly updated on all machines, including staff laptops used on the school network

- All email attachments are automatically scanned before they can be opened

- Children are not permitted to use Webmail in school

- Children must seek permission from a member of the school staff before downloading any files from the Internet

- All users will be made aware of copyright law and will acknowledge the source of any text, information or images copied from the Internet

- Children will be taught to conduct efficient searches for information and be reminded to use a common sense approach when using the Internet

- Children should be made aware of appropriate use of social media

Procedures for use of Instant Messaging (IM), Chat and Weblogs

- The use of instant messaging (e.g. MSN messenger) is not permitted in school. Staff will not engage with parent contacts who are only known to them through the school situation on social media

- Use of social-networking websites (e.g. Facebook and X) in school is not permitted except for use of the school's X and Facebook pages

- The above pages are only to be used by nominated members of staff. They are for sharing examples of children's work and links to the school blog. It must be monitored to ensure appropriate use

- Staff are not permitted to engage with pupils, parents or other interested parties on social network sites

- Pupils and staff must not access public or unregulated chat rooms in school but are permitted, however, to use regulated and educational chat environments

- Pupils and staff are permitted to join in educational forums which are moderated and hosted by a respectable organisation

- Use of weblogs is permitted for educational purposes only and must be supervised and pupils will be reminded of the safe practices and behaviours to adopt when posting material, as well as the need to adopt a formal and polite tone at all times

- The school recognises that children will use Instant Messaging, social-networking websites and weblogs outside school and aims to educate children into adopting safe practices on occasions when supervision is absent, whilst promoting awareness of the dangers of these new technologies amongst parents and carers

Procedures for Use of Cameras, Video Equipment and Webcams

- Parents who do not give consent for photographs of their children to be used in school, including on the website, must inform the school office

- Photographs or video footage will be downloaded or deleted and saved into a designated folder on the school network and this will be password protected and accessible only to authorised members of staff

- Any teachers or other members of staff must not use their own camera, video recorder or camera phone to take pictures of pupils or parents/carers

- Webcams must not be used for personal communication in school and should only be used with a member of staff present

- Pupils and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam and

the tone and formality of the language used must be appropriate to the audience and situation

Procedures to ensure safety of the school website

- The school has designated members of staff to lead the maintenance of the website. These are currently the ICT Co-ordinator (Mr Whaite) and the Bursar (Miss McGinty)
- The school website, blog and social media sites will be subject to frequent checks by the ICT Co-ordinator to ensure that no material has been inadvertently posted, which might put pupils or staff at risk
- Copyright and intellectual property rights must be respected
- Permission must be obtained from parents or carers before any images of children can be uploaded onto the school website
- Names must not be used to identify individuals portrayed in images uploaded onto the school website and if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear
- When photographs to be used on the website are saved, names of individuals should not be used as file names

Procedures for using mobile phones and Personal Digital Assistants (PDAs)

- Children are not permitted to have mobile phones in school, except in exceptional circumstances and in agreement with the headteacher. They will be stored at the parent's liability
- Staff must switch mobile phones off during lesson time
- Taking of pictures/videos using mobile phones in school is not permitted by staff or children
- Staff must not disclose mobile phone numbers to pupils

Procedures for using wireless games consoles

Pupils are not permitted to use games consoles in school or on school trips

Procedures for using Portable media players (e.g. iPods)

- Children are not permitted to bring in music players unless agreed by a member of school staff

- Use of media players in lessons is permitted for educational purposes

Sanctions to be imposed if procedures are not followed

- Parents contacted
- Details may be passed on to the police in more serious cases
- Legal action may be taken in extreme circumstances

Cases of misuse will be investigated by the school on an individual basis and appropriate sanction/s chosen.

Concluding Statement

Procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into schools.

(e-safety pol)