St George's CE Primary
E-safety Policy

Our Mission Statement

The example of Jesus Christ and the Good news that he brought inspire St George's school to be a caring and inclusive community in which **children love to learn and learn to love.**

Our view of the technology available to us

The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available. Use of email, mobile phones, Internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources. Virtual Learning Environments (VLEs) provide children and/or young adults with a platform for personalised and independent learning.

The benefits of having the technology available to the children in school

It enables children and/or young adults to be equipped with skills for the future as the Internet helps to improve children's reading and research skills. Email, Instant messaging and social networking helps to foster and develop good social and communication skills.

As a school we need to be aware of the dangers technology brings

Children might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails. Children might receive unwanted or inappropriate emails from unknown senders, or be exposed to abuse, harassment, terrorism or extremism material or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites, such as MySpace, Bebo, Facebook, etc. Chat rooms provide cover for unscrupulous individuals to groom children. Children will use the internet, emails, social networking and chat outside of school and it is essential that we equip them to keep safe by teaching digital literacy (e-safety) within school.

The positives far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours. This policy focuses on each individual technology available within the school and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

Procedures for Use of a Shared Network

- Staff must access the network using their own logons and passwords. These must not be disclosed or shared.
- Children must log on as themselves or as their year group (years – Rec, 1 and 2)
- Staff must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software should only be installed by the person responsible for managing the network (technician).
- Removable media (e.g. pen drives / memory sticks, CD-ROMs and floppy disks) must be scanned for viruses before being used on a machine connected to the network.
- Machines must never be left 'logged on' and unattended.
- Machines must be 'logged off' correctly after use.

Procedures for Use of Ipads

- All ipads are subject to the school filtering system. As the ipads can't be logged on, the filtering for the ipads defaults to the pupil filters.
- The ipads are supervised using lightspeed mobile device management.

Procedures for Use of the Internet and Email

- All users must sign an Acceptable Use Agreement before access to the Internet email is permitted in the establishment.
- Parental or carer consent is required in order for children to be allowed to use the Internet or email.
- Users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.
- The Internet and email must only be used for professional or educational purposes.
- Children must be supervised at all times when using the Internet and email.
- Procedures for Safe Internet use and sanctions applicable if rules are broken will be clearly displayed beside every computer with access to the Internet.
- Accidental access to inappropriate, abusive, terrorist, extremism or racist material is to be reported without delay to the person responsible for E-Safety (Mrs Walker) and a note of the offending website address (URL) taken so that it can be blocked by the technician.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.
- Internet and email use will be monitored regularly in accordance with the Data Protection Act.
- Users must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.
- Users must seek permission 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.
- All emails 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. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes.
- All email attachments must first be scanned before they can be opened.

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

- The use of Instant messaging (e.g. MSN messenger) is not permitted in school, *(unless permission to use this for a given educational purpose is granted**).*
- Use of social-networking websites (e.g. Bebo, MySpace, Facebook, Habbo, Piczo, etc.) in school is not permitted.
- Pupils and staff must not access public or unregulated chat rooms; Pupils and staff 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. This will 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

- **Permission must be obtained from a child's parent or carer before photographs or video footage can be taken.**
- Photographs or video footage will be downloaded immediately and saved into a designated folder on the school network.
- Any photographs or video footage stored on the school network must be deleted immediately once it is no longer needed or the children have left the school.
- Any teacher using their own camera, video recorder or camera phone during a school trip must transfer and save images and video footage into designated folder on the school network immediately upon return to school.
- Video conferencing equipment and webcams must be switched off (disconnected) when not in use (and the camera turned to face the wall).
- Webcams must not be used for personal communication in school and should only be used with a teacher 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. The tone and formality of the language used must be appropriate to the audience and situation.

Procedures to ensure safety of the school website

- **All content and images to be published on the school website will be approved by a designated member of staff prior to it being published.**
- The school website will be subject to frequent checks to ensure that no material has been inadvertently posted, which might put the pupils or staff at risk.
- **Copyright and intellectual property rights will be respected.** Permission will be requested before any files or materials created or owned by another person or company are used.
- **Permission will be obtained from parents or carers before any images of children can be uploaded onto the school website.**
- Children's names will not be used with their photographs on the school website

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

- Children are required to hand in their mobile phones into the class teacher at registration and collect them at hometime.
- Staff are required to switch mobile phones off during lesson times. The making and receiving of phone calls during this time, as well as the sending or receiving of text messages is banned.

Procedures for using wireless games consoles and Portable media players (e.g. iPods)

- Wireless, handheld games and portable media players are banned from school.
- Any unwanted contact, which makes children feel vulnerable or uncomfortable, must be reported immediately to an adult.

Latest review Spring term 2018

To be reviewed as required and presented to Governors at least annually

Appendix 1

E-Safety (Digital Literacy) is taught as part of the Computing curriculum. It can be taught at any time during the year but there is a particular focus on it during the first half of the Autumn Term(start of School Year); around Safer Internet Day (usually early February) and the end of the Summer Term to encourage pupils to stay safe during the Summer Holidays.

The school uses the Smart Rules

S	Safe	Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.
M	Meeting	Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.
A	Accepting	Accepting emails, IM messages or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages.
R	Reliable	Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.
T	Tell	Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Useful websites to support the teaching of e-safety include

www.thinkuknow.co.uk
www.childnet.com
www.kidsmart.org.uk