Respect *For All* | **Ambitious** *In Aspirations* | **Bold** *In Actions*

"...with God all things are possible" Matthew (19:26)

E-Safety policy

Completed by:	**John Lucas**
Date completed:	**February 2024**
Agreed by governors:	**Summer 2024**
To be reviewed:	**Summer 2025**

Contents

At St Georges C of E Primary School we understand the responsibility to educate our pupils in e-Safety issues, teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites;
- Learning Platforms and Virtual Learning Environments;
- Email and Instant Messaging;
- Chat Rooms and Social Networking (Facebook, WhatsApp, Skype etc.);
- Blogs and Wikis;
- Podcasting;
- Video Broadcasting;
- Music Downloading;
- Gaming;
- Online gaming;
- Mobile/ Smart phones with text, video and/ or web functionality; Other mobile devices with web functionality (e.g. tablets).

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At St Georges C of E Primary School, we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-coordinator in our school is Miss Law who has been designated this role as she is also the Computing Co-Ordinator. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety co-coordinator to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection) and Child net. Senior Management and Governors are updated by the Head / e-Safety coordinator and all governors understand the issues and strategies at our school in relation to local and national guidelines and advice. This policy is linked to the following mandatory school policies: child protection, safeguarding, health and safety, home–school agreements, and behaviour/pupil discipline (including the ant bullying) policy and PHSE.

E-Safety skills development for staff

Our staff receive regular information and training on e-Safety issues in the form of updates at staff meetings, correspondence from co-ordinator;

- New staff receive information on the school's acceptable use policy as part of their induction;

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community;
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas. Managing the school e-Safety messages
- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used;
- The e-Safety policy will be introduced to the pupils at the start of each school year;
- E-Safety posters will be prominently displayed.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. e-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.
The school has a framework for teaching internet skills in Computing/ PHSE lessons;
The school provides opportunities within a range of curriculum areas to teach about e-Safety including the dangers of social network sites;

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum;
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them;
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities;
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Child line/ CEOP report abuse button.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security and these points for how to create a strong password.
A strong password Should be:

- At least 12 characters long but 14 or more is better

- A combination of uppercase letters, lower case letters, numbers and symbols
- Not a word that can be found in a dictionary or the name of a person, character, product or organisation.
- Significantly different from your previous passwords.
- Easy for you to remember but difficult for others to guess. Consider using a memorable phrase like"6MonkeysRlooking^".

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety policy;
- The Child Friendly E-safety Policy has been shared with both pupils and parents.
- Users will be provided with an individual network, email and Learning Platform log-in username;
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others;
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared. Individual staff users must also make sure that workstations are not left unattended and are locked;

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008).
Staff are aware of their responsibility when accessing school data. Level of access is determined by the HT;

- Any data taken off the school premises must be encrypted Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data
- Managing the Internet
- The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All Whenever any inappropriate use is detected it will be followed up.
- The school will provide supervised access to Internet resources (where reasonable) through the school's fixed & mobile internet technology;
- Staff will preview any recommended sites before use;
- Raw image searches are discouraged when working with pupils;
- If Internet research is set for homework, specific sites will be suggested that

have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research;

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources;
- All users must observe copyright of materials from electronic resources.
- School internet access is controlled through the LA's web filtering service.
- St George's C of E Primary School is aware of its responsibility when monitoring staff communication under current legislation and considers; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998;
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required;
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-Safety co-ordinator;
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines;
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the Computing co-coordinators to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media, it must be given to the teacher for a safety check first;
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Head teacher/Computing Co –Coordinator
- If there are any issues related to viruses or anti-virus software, the Computing coordinator should be informed and then inform the technician and technical support team for support.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of

these devices in the following ways so that users exploit them appropriately.
Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device;
- Pupils are not allowed to bring personal mobile devices/phones to school. However, if a pupil is found to have a mobile device the device will need to be given to the office and placed in a class "phone box" for safe keeping until the end of the school day. The school is not responsible for the loss, damage or theft of any personal mobile device;
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. School provided Mobile devices (including phones)
- The sending of messages that intend to threaten, cause harm or make the reader uncomfortable in any way between any member of the school community is not allowed;
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community;
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used;
- In cases where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good „netiquette". In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed;
- Staff must use the official school e-mail system for work e-mails;
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business; • Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses;

- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper;
- staff sending emails to external organisations, parents or pupils are advised to cc. the Head teacher, line manager or designated account;
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes;
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments;
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail;
- Staff must inform (the e-Safety co-ordinator and Head teacher) if they receive an offensive e-mail;
- Pupils are introduced to Email in the Teach Computing Curriculum.

Safe Use of Images

Taking of Images and Film Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment;

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device;
- Publishing pupil's images and work On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:
  - on the school web site;
  - in the school prospectus,
  - newsletter and other printed publications that the school may produce for promotional purposes; recorded/ transmitted on a video or webcam;
  - in display material that may be used in the school's communal areas;
  - in display material that may be used in external areas, i.e. exhibition promoting the school;
  - general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

- and on Class Dojo pages.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils‟ names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils‟ full names will not be published.

Before posting student work on the internet or Class Dojo, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Web Manager has authority to upload to the site.

- Storage of Images
- Images/ films of children are stored on the school's equipment;
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head teacher; • Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network;
- The staff have the responsibility of deleting the images when they are no longer need—IE when the children have left.

Misuse and Infringements
Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Head teacher. Incidents should be logged. Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinator;
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Users are made aware of sanctions relating to misuse or misconduct. All staff are aware of the policy and the children have signed an acceptable use policy.
- access to computer files or software without permission (for example using another person's password to access files);
- unauthorised access, as above, in order to commit a further criminal act (such as fraud); • impair the operation of a computer or program.

Equal Opportunities

Pupils with additional needs: the school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools" e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school. We regularly consult and discuss e-Safety with parents/ carers on Class Dojo and seek to promote a wide understanding of the benefits related to ICT and associated risks. Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Parents/ carers are required to decide as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website) The school disseminates information to parents relating to e-Safety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website/ Learning Platform postings
- Newsletter items
- Learning platform training

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them. This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Miss Law the school e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed „reasonable" by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business. I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of AVA/ Head Teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that any personal social media are set to private to ensure that pupils/parents do not inadvertently have access to any private or personal details.

- I will not invite or accept a child or a parent as a "friend" on Facebook or other social networking site.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature _____ Date _____

Full Name _____(printed)

Job title _____

Primary Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT in school for school purposes.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is

responsible, polite and sensible.

- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety
- I will not any under any circumstances join Facebook as I am not 13 years old.

Name _____
Date_____
Class _____