SAINT JOHN'S

E-Safety and Acceptable Use Policy

Designated Member of Staff	Deputy Head Teacher
Committee with responsibility	Curriculum and Standards
Date of Issue	Autumn 2021
Frequency of Review	Annual

Issue Number	Issue Date	Summary of Changes
1	December 2021	Re-formatting of the policy
2	May 2023	Review of policy

Policy Statement

This policy reflects the Christian Values and philosophy of Saint John's Church of England Primary School that the school is a place "where we all flourish".

The e-Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents

Safeguarding is a serious matter. At Saint John's Primary we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-Safety is an area that is constantly evolving and as such this policy will be reviewed every year or in response to an e-Safety incident.

The primary purpose of this policy is two-fold:
• To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
• To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

How will the risks be assessed?
In common with other media such as magazines, books and video, some material available via the Internet/devices is unsuitable for pupils. Staff will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a workstation. The school cannot accept liability for the material accessed, or any consequences thereof. We use SWGFL filtering service.

How will pupils be taught to assess Internet content?
• Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
• Pupils will be taught to validate information before accepting it as true, an important aspect of higher levels of subject teaching.
• When copying materials from the Web, pupils will be taught to observe copyright to avoid plagiarism.
• Pupils will be made aware that the writer of an email or the author of a Web page may not be the person claimed.
• Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV.

Cyber-Bullying
Cyber-bullying is using technology to hurt other people and is repeated over time. At Saint John's, we ensure safe use of technology through rigorous security settings and close monitoring.

• Cases of cyber bullying will be dealt with individually, seriously and immediately.
• This policy will be used in conjunction with the Behaviour Policy, Anti-Bullying Policy and the Safeguarding Policy.
• Activity that threatens the integrity of the school IT system, or activity that attacks or corrupts other systems, is forbidden.
• Users are responsible for all emails sent and for contacts made that may result in email being received.

Governing Body
The governing body is accountable for ensuring that our school has effective policies and procedures in place, They will:
• Appoint one governor to have overall responsibility for the governance of e-Safety at the school who will keep up to date with emerging risks and threats through technology use and receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
• An annual meeting will be used to discuss current policy and practice.

Headteacher
Reporting to the governing body, the Headteacher has overall responsibility for e-Safety within our school.

The Headteacher will ensure that:
• E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
• All e-Safety incidents are dealt with promptly and appropriately.

Deputy Headteacher
Ensuring all hardware and software is appropriately and prepared ready for all users and liaising with our technical support, Focus Networks, to ensure smooth running of all technology throughout the school.

They will:
• Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
• Review this policy regularly and bring any matters to the attention of the Headteacher.
• Advise the Headteacher and governing body on all e-Safety matters.
• Engage with parents and the school community on e-Safety matters at school and/or at home.
• Liaise with the local authority and other agencies as required.
• Ensure e-Safety incidents are added to our Safeguarding logging programme, 'CPOMS'. Ensure staff know what to report and ensure the appropriate audit trail.
• Ensure any technical e-Safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
• Make themselves aware of any reporting function with technical e-Safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-Safety incident is reported to the Deputy Headteacher or Headteacher and added to CPOMS.
- All staff annually sign the Staff Acceptable Use Agreement sheet. Copies to be kept in personnel files in the office.

All Pupils

The boundaries of use of IT equipment and services in this school are given in the Pupil Acceptable Use Agreement sheet which is signed at the beginning of each academic year. Any deviation or misuse of IT equipment or services will be dealt with in accordance with the Behaviour and Anti-Bullying Policies.

E-Safety is embedded into our curriculum. Pupils will be given the appropriate advice and guidance by staff. Whenever devices are used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupils' learning. Similarly, all pupils will be fully aware of how they can report areas of concern whilst at school or outside of school. See Anti-bullying Policy.

The use of personal devices by children, such as mobile phones, are not allowed on the school site, unless in specific scenarios where children may walk to and from school without parental supervision. This is reviewed and accepted on a case-by-case basis and, if brought into school, mobile phones are immediately handed over to the teacher to be kept in a locked cupboard before being returned at the end of the day.

Parents and Carers

Parents play the most important role in the development of their children and as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through the website and school newsletters, the school will keep parents up to date with new and emerging e-Safety risks and will involve parents in strategies to ensure that students are empowered.

Technology

Saint John's uses a range of devices. In order to safeguard the students and in order to prevent loss of personal data, we employ the following assistive technology:
Internet Filtering – we use SWGFL filtering service that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner.

The Computing Coordinator, Deputy Headteacher and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use Office 365 SPAM software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Anti-Virus – All capable devices will have anti-virus software. Our Anti-Virus updates regularly and removes threats as soon as they are spotted. IT support (Focus Networks) will be

responsible for ensuring this task is carried out correctly, and will report to the Deputy Headteacher if there are any concerns.

All staff, pupils and parents of pupils will be informed that internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Posting anonymous messages and forwarding chain letters is forbidden. As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.

Photos and videos –. All parents must sign a media release slip. Photos and videos may only be taken on school devices and not personal devices owned by staff unless by prior permission.

Social Networking – The school has agreed social networks that are used for communicating with parents.

In addition, the following is to be strictly adhered to:
• Permission must be consulted before any image or video of any child is uploaded.
• All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, the Headteacher will ensure that all appropriate staff at Saint John's Primary School will have an annual programme of training which is suitable to the audience. We regularly review guidance given to parents on e-Safety and information of which is available on the school website.

During e-Safety lessons children will be informed that their internet activity may be monitored and will have a chance to voice opinions/ask questions.

At the beginning of each new academic year, staff have agreed to discuss the following agreement/e-safety rules at an age appropriate level with their class. Once understood, pupils can then sign the attached sheet. The completed agreement should then be displayed in each class.

Pupil Acceptable Use Agreement

- ✓ I will conduct myself online in line with the Christian values.
- ✓ I will only use IT in school for school purposes.
- ✓ I will only use a teacher agreed email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will only download programs and files that my teacher has agreed to.
- ✓ I will not tell other people my passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all IT contacts 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 not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using IT 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 IT can be checked and that my parent/carer may be contacted if a member of school staff is concerned about my e-Safety.

Sign on this page to accept that you have read, understood the 'Pupil Acceptable Use Agreement' and will adhere to all points.

Staff Acceptable Use Agreement

This agreement reflects the Christian Values and ethos of Saint John's CE Primary School in relation to staff use of IT.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and support awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of IT in their everyday work.

The school will ensure that staff and volunteers have good access to IT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of IT. I will educate the young people in my care in the safe use of IT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (eg laptops and email) out of school.
- I understand that the school IT systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school IT systems.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities. This will include not inviting pupils onto personal social networking sites.
- Where possible I will use a school camera (where a personal device is used, any images should be downloaded onto a secure school system immediately and then deleted)

In classes where Class Dojo, Tapestry or other web-based communication software or apps are used, parents and staff sign a user agreement to clarify acceptable terms of use.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of school.

I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include, a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.