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
3	June 2024	Review of policy, re-written and ratified in Term 6

New technologies have become integral in today's society, both within schools and 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.

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 term E-Safety refers to children being safe when using technology, particularly when online.

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.

Online Safety at Saint John's
Email Filtering – we use Office365 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 will 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 from the Headteacher.

Social Networking – The school has agreed social networks that are used for communicating with parents. Any personal social media accounts of members of staff should be made private and staff should not connect, follow, send messages to or accept requests from families using personal social media accounts. Contact with families of pupils online should be restricted to using in-school programs such as: Class Dojo.

In addition, the following is to be strictly adhered to:
• Parents 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. 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 is monitored all the time; they will have a chance to voice opinions/ask questions.

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. South West Grid For Learning (SWGFL) provide our school filtering service. 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.

How will pupils be taught to assess the internet?

- The Computing curriculum directly teaches children of all ages to access content online appropriately and safely. The PSHE curriculum also covers aspects of e-safety and cyber-bullying. This is supplemented by regular conversation and discussion with classrooms about positive use of ICT equipment, software, apps and the internet. This means pupils are directly taught how to stay safe online and all staff promote this. Please refer to our Computing Subject Policy for a detailed outline of explicit teaching of e-safety.
- Annually, school will further emphasise the importance of staying safe online through a dedicated 'Safer Internet Day'.
- Pupils read and sign a pupil acceptable use agreement at the beginning of each new academic year to show they understand the expectations when using school equipment. This agreement (Appendix A) details how pupils are expected to conduct themselves and further explains how pupils are taught to access the internet safely.

Cyber-Bullying

Cyber-bullying a repeated, deliberate and targeted act which physically or emotionally harms another person, usually involves an imbalance of power and is done several times on purpose using technology. Technology plays a huge part in today's society and in the lives of children; we acknowledge that this means Cyber-bullying will need particular attention within this policy.

- This policy will be used in conjunction with the Behaviour Policy, Anti-Bullying Policy and the Safeguarding Policy to keep all members of the Saint John's community safe.
- Any cases of cyber-bullying will be dealt with individually, seriously and immediately.
- 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 content sent by them.

Cyber-bullying behaviours can be, but are not limited to:

- Abusive comments, rumours, gossip and threats made via digital communications and/or technologies - this includes internet gaming.
- Sharing pictures, videos or personal information without the consent of the owner and with the intent to cause harm or humiliation.
- Hacking into someone's email, phone or online profiles to extract and share personal information, or to send content while posing as that person.
- Creating social media accounts, pages, chat rooms and posts that intend to harm, make fun of someone or spread malicious rumours.
- Pressurising someone to do something online they do not want to do such as sending personal images.

Ways we support pupils who experience cyber-bullying and their families:

- Encouraging them to keep copies of anything that may be regarded as cyber-bullying.
- Discussing with pupils who demonstrate cyber-bullying behaviours the impact of their actions and reminding them of the legal implications of their actions.
- Talking with families about these issues and how online activity can be monitored and supervised at home.

We also use these strategies to prevent cyber-bullying:

- Regular online safety lessons.
- Reminding pupils of safe internet use during computing lessons.
- Promotion of online safety in assemblies.
- Rigorous security settings and close monitoring of online activity in school.
- Making online safety information available on the school website and Class Dojo.
- Promoting websites and advice to parents which support parents in keeping children safe online.

Pupils who are vulnerable to experiencing bullying behaviour and to demonstrating bullying behaviours include those experiencing:

- Personal insecurity or worries *(they may be concerned about others judging them, picking on them or pointing out failings).*
- Loss of power or status *(they could experience bullying themselves).*
- Challenging personal circumstances *(for example, trauma, family relationships…).*
- Lack of knowledge or understanding of others *(such as not knowing that some jokes or comments may hurt some people and not others).*
- Difficulties with accepting unique qualities in others (*such as physical, cultural, social, financial, learning, developmental or sexual differences).* They may have these unique qualities and need the support of others to feel accepted and included.

The following strategies help school to identify incidents of bullying:

- All staff watch for early signs of changes in behaviour and attitudes of pupils.
- All staff listen, believe and investigate.
- Establish with all pupils the school's definition of bullying and the behaviours that are linked with bullying.
- Encourage pupils and parents to inform staff members of concerns regarding bullying behaviour.
- Provide different ways for pupils to raise concerns comfortably regarding bullying behaviour.
- Display the Childline telephone number around school and in each classroom.

The role of different stakeholders:

Families

Family members play the most important role in the development of their children and as such the school will ensure that key family members 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 family members up to date with new and emerging e-Safety risks and will involve key family members in strategies to ensure that students are empowered.

Families will:

- Work with school to ensure that children are kept safe online by engaging with training sent home or led by school.
- Monitor their child's online activity.
- Ensure their child is not exposed to content or technology before it is appropriate for them.
- Support and trust the school when dealing with any e-Safety-related incidents that may occur involving their child.

The governing body will:

- Ensuring that our school has effective policies and procedures in place, discussing and reviewing these annually.
- 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.

The Headteacher will:

- Have overall responsibility for e-Safety within our school.
- Ensure e-Safety training throughout the school is planned, up-to-date and appropriate for the recipient, i.e. pupils, all staff, the governing body and parents.
- Ensure all e-Safety incidents are dealt with promptly and appropriately and reported to the governing body.
- Ensure all staff have signed the Acceptable Use agreement annually.

The Deputy Headteacher will:

- Ensure all hardware and software is appropriate and prepared ready for all users
- Liaise with our technical support, Focus Networks, to ensure smooth running of all technology throughout the school.
- 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 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:

- Must annually read and sign the Staff Acceptable Use Agreement which can be found at the end of this policy. Record of signatures to be kept in personnel files in the office.
- 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 Pupils will:

- Sign and agree to follow the expectations outlined in the Pupil Use Agreement every year.

Any deviation or misuse of IT equipment or services will be dealt with in accordance with the Behaviour and Anti-Bullying Policies.

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.

Pupil Acceptable Use Agreement

- ✓ I will use school equipment appropriately and sensibly for school purposes.
- ✓ I will only use the internet or apps in school when an adult has given me permission.
- ✓ I will tell an adult if I see something that makes me feel unhappy, scared, worried or uncomfortable on any school equipment.
- ✓ I will not share any personal information about myself or others online.
- ✓ I will not tell other people my passwords.
- ✓ I understand that the internet contains information that can be written by anyone and it may not always be true.
- ✓ I can use trustworthy and reliable sources to find information online.
- ✓ I will only open, work on or delete my own files.
- ✓ I will be kind, caring to myself and others when using the internet.
- ✓ I know that my use of school equipment is monitored and checked.
- ✓ I know that my parent/carer may be contacted if a member of school staff is concerned about my e-Safety.

Class Dojo

Class Dojo is a digital classroom management tool, used as a method of sharing information, communication between school and home and keeping families up to date with what is going on in school. Access to Class Dojo is restricted to children, family members and staff. Parents must sign a form to consent their children to be present and included in photos and videos that may be shared on Class Dojo. Teachers may use Class Dojo's 'Class Story' feature to share photos or information about exciting events their children are involved in at school or general messages to all parents. Parents are able to contribute towards this class story by viewing the posts uploaded by the teachers and sending in work or events that children have taken part in at home, which can then be uploaded by the teacher if appropriate. Parents and teachers may use the 1:1 messaging format to communicate directly, however all messages must be appropriate, polite and formal. Please refer to the Class Dojo Policy on our school website for further details.

Please see below a poster which outlines expectations for all staff, children and family members.

Dos	Don'ts
√ Treat the messages as professional emails, rather than text messages or social media e.g. emojis. √ Ensure all questions and comments are pertinent to your child. √ Please check regularly as we post updates. We strive to give as much notice as possible but sometimes things can change quickly. √ Share in-school and out-of-school learning and achievements e.g. musical instrument exams.	X - Use Class Dojo to report your child as absent. Please contact the school office directly. X - Post comments as complaints about the school or teachers. Please refer to policies on our school website for this. ClassDojo

Staff aim to respond to messages received within 24 hours but please be patient; we often do not look at Class Dojo during the school day and regular meetings, marking and staff work-life balance can mean we do not get a chance to look at them until the next day.

If you have a question, query or concern, your child's class teacher (rather than the TA) is your first port of call. If your message is urgent, please speak to the office directly.

Staff Acceptable Use Agreement

This agreement covers the requirements for all staff when using technology in school, both equipment provided by school (e.g. staff laptop) and equipment brought into school from home (personal mobile phone).

The aims of this Acceptable Use Agreement are:

- to ensure staff will be responsible in their use of school and personal equipment and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- to ensure that school staff understand the impact of not using technology and equipment appropriately and ensure that staff avoid potential risks in their use of technology at all times.

Using technology:

- I will only use equipment which has been permitted for my use by the Head Teacher.
- I will share information and communicate about work-related matters using only my individual school email address.
- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will take care of all equipment provided by school and take measures (e.g. using provided laptop covers) to avoid them becoming damaged.
- I will back up my files and data regularly.
- I will delete, without opening, emails which contain links, websites or attachments where I am unaware of the source. I will not open or reply to emails that have been sent from unknown senders. I will ask for support if I am unsure of the sender or source of emails before acting.
- I will not share school-related usernames or passwords with staff, parents or pupils unless permission has been given.
- I will not attempt to use others' school-related usernames or passwords, unless permission has been given.
- I will only use approved and recommended removable media (e.g. encrypted memory sticks) and will keep these safe.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Head Teacher.
- I will immediately report any damage or faults involving equipment or software.
- I will not access, copy, remove or otherwise alter any other users' files, without their permission.
- 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.

Mobile Devices

- Where possible I will use a school device (e.g. camera, iPad) to take photos and videos of school-related activities.
- In the rare occasion when a school device is not available, I will obtain permission from the Head Teacher to use a personal device before any action is taken. If permission is granted, any images must be downloaded onto a secure school system as soon as possible and then deleted.

- I will only use my mobile phone for personal use during out of school hours, unless permission has been given by the Head Teacher. This includes during INSET days, training and staff meetings.

Social Media & Professionalism

- I will not engage in any on-line activity that may compromise my professional responsibilities.
- 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 be professional in my communications with others at all times.

Use of internet, software or apps

- I will only use the internet for personal use during out-of-school hours.
- I will not install any software onto my school devices without permission to do so.
- I will ensure that any children present in photographs and videos put on public forums (e.g. Class Dojo, School Website) have consent from parents and carers prior to upload.
- I will not search for, download, upload, view or access illegal, inappropriate content or content that may cause harm or distress to others in any way.
- 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 the statements set out in this agreement apply to my use of school ICT systems in and out of school as well as 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: warning, suspension, referral to Governors and / or the Local Authority and, in the event of illegal activities, the involvement of the police.