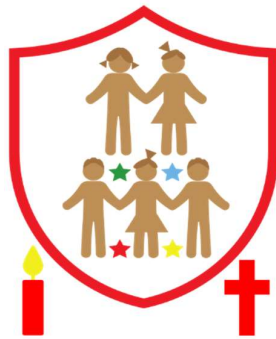


# St James' Church of England Junior School

Developing the love of life and learning in a  
caring Christian community



## E-SAFETY POLICY

September 2020

**Reviewed by:** Justin Hutchinson  
**Agreed by FGB:** 14<sup>th</sup> September 2021  
**Review Cycle:** Annually  
**Next Review due:** September 2022 – Extended to 31<sup>st</sup> November 2022

## **Policy Statement**

At St James' C of E Junior School 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 on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to entrust the whole school community with the ability to stay safe and risk free.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce the potential of harm to the pupil or liability to the school.

This policy is available for anybody to read on St James' C of E School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy Pupils E-Safety agreement will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

## **Introduction**

Information Technology (IT) in the 21<sup>st</sup> 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. Schools need to build in the use of these technologies in order to enable our young people with the skills to access life-long learning and employment.

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

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of:

- Fixed Internet (LAN and WiFi).
- Mobile Internet
- Technologies provided by the School (such as PCs, laptops, iPads, tablets, webcams, whiteboards, digital video equipment, etc).
- Technologies owned by pupils and staff, but brought onto school premises (such as laptops, tablets, mobile phones, camera phones, PDAs and portable media players, etc).

## **Policy Governance (Roles & 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-ordinator in our school is Mrs A Anderton. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety co-ordinator

to keep abreast of current issues and guidance through organisations such as LEA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Teaching staff and Governors are updated by the Head / E-Safety co-ordinator and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy. In addition, it is to be read in conjunction with General Data Protection Regulation (GDPR).

### **Why is Internet use important?**

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
- The school has a duty to provide students with quality Internet access as part of their learning experience
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security

### **How does the Internet benefit education?**

- Access to world-wide educational resources including museums and art galleries; inclusion the National Education Network which connects all UK schools
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the LEA (Local Education Authority) and DfE (Department for Education)
- Access to learning wherever and whenever convenient

### **How can the Internet enhance learning?**

- The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and ability

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluated.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the Computing Subject Leader Justin Hutchinson, and/or the school's ICT technician.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
- Pupils should be taught to be aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of on-line materials is a part of every subject

#### **How will ICT system security be maintained?**

- The security of the school ICT systems will be reviewed regularly
- Virus and ransomware protection will be installed and updated regularly
- Personal data sent over the Internet will be encrypted or otherwise secured
- Use of portable media will be reviewed. Portable media may not be used without specific permission and a virus check
- Files held on the school's network will be regularly checked
- The ICT co-ordinator / ICT technician will review system capacity regularly
- Personal external storage devices and CD/DVD's brought in by staff or pupils should not be used without the Headteacher's permission and should be scanned for viruses / malware before use on the school's system.

#### **How will e-mail be managed?**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Year 6 children will have their own email address; this will be deleted on their leaving school
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters / emails is not permitted

#### **How will published content be managed?**

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright

#### **Can pupil's images or work be published?**

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents. Written consent will be obtained from children's parent or guardian

### **How will social networking and personal publishing be managed?**

- The school will block/filter access to social networking sites
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. House number, street name, school, shopping centre.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others
- Pupils should be advised not to publish specific and detailed private thoughts
- We are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments
- The school's PRHE scheme of work has been extended to incorporate the education of children on the Internet and its safe use

### **How will filtering be managed?**

- Internet Filtering is provided by South West Grid for Learning (SWGfL)
- We will work in partnership with parents, the LEA, DfE, SWGfL and our ICT support provider to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the ICT co-ordinator or ICT technician. Children will be educated as to the correct and safe procedure to do this
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be referred to the Internet Service Provider.
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate

### **How can emerging technologies be managed?**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is permitted
- Staff will be issued with a school phone where contact with pupils is required

### **How should personal data be protected?**

The Data Protection Act 2018 (encompassing GDPR) requires that data is:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries / parties with suitable security measures

### **How will Internet access be authorised?**

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn
- Our pupils' access to the Internet will be by adult demonstration with opportunities for the children to work directly on the Internet individually or with a partner. This will always be directly supervised by a teacher or adult
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form

### **How will risks be assessed?**

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly
- The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored

### **How will e-safety complaints be handled?**

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headteacher
- Pupils and parents will be informed of the complaints procedure
- Parents and pupils will need to work in partnership with staff to resolve issues

- Discussions will be held with the Police liaison officer to establish procedures for handling potentially illegal issues
- The Safer Internet police agency will be informed of any potentially unsafe practice.
- CEOPs referral may be made if there is a possibility of exploitation e.g. grooming

#### **Sanctions within the school discipline policy include:**

- interview / counselling by teacher / Headteacher;
- informing parents or carers;
- police may be informed;
- removal of Internet or computer access for a period of time.

#### **How is the Internet used across the community?**

- The school will liaise with local organisations to establish a common approach to e-safety
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice

#### **How will the policy be introduced to pupils?**

- Rules for safe Internet access will be posted in all areas of the school with access to the internet. These rules will be carefully written and illustrated to ensure all children understand their message. Children from the School Council will be involved to ensure these rules are approved by children, for children
- Pupils will be informed that Internet use will be monitored
- An E-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use. Instruction in responsible and safe use should precede Internet access. When this policy is released to pupils, staff, parents, the internet will be out of bounds until consent has been received
- Responsible Internet use is incorporated into Computing units of work, covering the following strands: Self-image and identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, well-being and lifestyle, Privacy and security and Copyright and ownership.
- The school will work with Gloucestershire Safeguarding partners to access resources, including 'In the Net' performance

#### **How will the policy be discussed with staff?**

- All staff must accept the terms of the 'Acceptable Use Policy' statement before using any Internet resource in school
- All staff will be given the School E-Safety Policy and its importance explained to them. The whole staff will also be involved in the confirmation of the final draft of this policy before release to parents and children
- Staff will be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- The monitoring of Internet use is a sensitive matter. Members of staff that operate monitoring procedures should be supervised by senior management and members of the E-Safety committee

- Staff development in safe and acceptable use of the Internet and on the school E-Safety Policy will be provided as required

**How will parents' support be enlisted?**

- Parents' attention will be drawn to the School E-Safety Policy in initial letters and newsletters and from then onwards; the school website
- Internet issues will be handled sensitively to inform parents without alarm
- A partnership approach with parents will be encouraged. This includes a monthly up-to-date online safety newsletter which is emailed to parents.





# St James'

## Church of England Junior School

Developing the love of life and learning in a caring Christian environment

### Pupils' E-Safety Agreement

#### For my own personal safety – everywhere!

- I will only use IT equipment when instructed to do so.
- I will ask permission from a member of staff before using the Internet at school.
- I am aware of “Stranger Danger” and will not agree to meet online friends.
- I will tell an adult about anything online that makes me feel uncomfortable or unsure.
- I will not try to reach websites the school has blocked.
- I understand that the school may check my files and may monitor the web pages I visit.
- When in school I will only contact people with my teacher's permission. I will be very careful when sharing pictures or video of myself or my friends. If I am in school, I will always check with a teacher.
- I will not put any of my “Personal Information” online. (My full name, birthday, phone number, address, postcode, school etc.)

#### To keep the system safe

- I will only use my own login and password, which I will not let anyone else know.
- I will not access other people's files.
- I will not play games on a school computer unless my teacher has given me permission.
- I will not install software on school computers.
- I will not attach any equipment to the school computers, such as memory sticks.
- I will not use the system for gaming, gambling, shopping, or uploading videos or music.

#### Responsibility to others

- The messages I send will be polite and responsible.
- I will not upload images or video of other people without their permission.
- Where work is copyrighted (including music, videos and images,) I will not either download or share with others.
- I understand that the school may take action against me if I am involved in inappropriate behaviour on the internet and mobile devices.

## **Personal Devices**

- The school cannot accept responsibility for loss or damage to personal devices.
- It is not permitted for pupils to use Mobile Phones during the school day. Mobile phones should not be brought into school unless there is a genuine reason for doing so and my parents have approved this.
- If I have to bring my mobile phone into school, I will hand it to the Family Support Worker at registration and get it back at the end of the school day.
- Other devices (e.g. Games consoles, cameras) should not be brought into school, unless my teacher has given me permission.



# St James' Church of England Junior School

## Pupils E-Safety Contract

Please complete, sign and return to the class teacher.

Pupil:

Class:

### Pupil's Agreement

I have read and I understand the pupils e-safety agreement, and will abide by the rules which are designed to keep both myself and the school safe

Signed:

Date:

### Parent's Consent

I have read and understood the e-safety agreement and give permission for my son / daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on e-safety at school, advice for parents is available at [www.saferinternet.org.uk](http://www.saferinternet.org.uk) or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I will ensure that any pictures taken during school events that include other children will not be shared using social media.

Signed:

Date:

Please print name: