St John's Church of England Academy

E-Safety Policy

Agreed	**April 2015**
Adopted	**April 2015**
Next Review	**Spring 2018**

St John's Church of England Academy

E-Safety Policy – April 2015

RATIONALE:

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. Pupils with internet access are more confident and have been shown to produce better-researched, more effective and well presented projects.

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies.

While many of the issues outlined in this section relate, primarily, to ICT use outside school, it is inevitable that some of the issues, when initiated outside school, will be bought back in and need to be dealt with accordingly by the school. For example, bullying via chat or text messages will impact upon relationships within school; obsessive use of the internet may impact upon the quality of schoolwork.

Schools therefore have a major responsibility to educate their pupils; 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.

E-SAFETY ROLES

WHO WILL WRITE AND REVIEW THE POLICY?

- The school will appoint an e–Safety Coordinator. This is usually the ICT Coordinator who will work alongside the designated Child Protection / Safeguarding Officer as the roles overlap.
- The e–Safety Policy and its implementation will be reviewed annually by the E-Safety coordinator.

TEACHING AND LEARNING

WHY IS INTERNET USE IMPORTANT?

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- 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 functions.

HOW DOES INTERNET USE BENEFIT EDUCATION?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- 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 across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

HOW CAN INTERNET USE ENHANCE LEARNING?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils will comply with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

HOW WILL PUPILS LEARN HOW TO EVALUATE INTERNET CONTENT?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

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.

TECHNICAL INFORMATION

HOW WILL INFORMATION SECURITY SYSTEMS BE MAINTAINED?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Technical support will be provided by ITSS.

HOW WILL EMAIL BE MANAGED?

- Pupils may only use approved email accounts which are set up to only accept internal mail only.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school.

CAN PUPILS IMAGES OR WORK BE PUBLISHED?

- Images that include pupils will be selected carefully and will not provide material that could be reused.
- 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 images of pupils are electronically published.

HOW WILL SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING BE MANAGED?

- The school will control access to social media and social networking sites and in most cases these website are blocked by our filtering system.
- Pupils will be taught never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Details of the specific e-safety skills to be taught at different year groups is to be found in Appendix 3.

HOW WILL FILTERING BE MANAGED?

- The school will ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e–Safety Coordinator.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- Filtering systems will be maintained by ITSS and any changes will be arranged through them.

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 allowed.
- Staff will use a school phone where contact with parents is required.
- Mobile phones will not be used during lessons or formal school time unless there is a specific education benefit. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

HOW WILL INTERNET ACCESS BE AUTHORISED?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the Staff Acceptable Use form.
- At Key Stage 1, access to the Internet will be by adult demonstration with directed access to specific, approved on-line materials.
- Parents will be asked to sign and return a Pupil Acceptable Use form on joining the school.

HOW WILL RISKS BE ASSESSED?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- Children are taught to be critically aware of the websites and information they access using the Internet. There are reporting procedures in place to deal with any of these instances. This is re-enforced with the pupils during e-Safety lessons.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The school will monitor pupils' internet use, as far as practically possible, to minimise the risk of pupils being involved in or coerced into inappropriate behaviour. These may include but are not limited to cyber-bullying, sexting, playing inappropriate video games, potential radicalisation or grooming.

E-SAFETY INCIDENT REPORTING

HOW WILL E-SAFETY INCIDENTS BE HANDLED?

- Instances of Internet misuse will first be reported to the ICT co-ordinator who will then refer these to the Head Teacher. The Head Teacher will then deal with this as per the Child Protection Policy.
- Any complaint about staff misuse must be referred to the Head Teacher. This will then be dealt with as per Employee Code of Conduct.
- All e–Safety complaints and incidents will be recorded by the school using the E-Safety Incident Report form which details the incident and any actions taken.

HOW WILL CYBER BULLYING BE MANAGED?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by Cyberbullying.

POLICY REVIEW

HOW WILL THE POLICY BE INTRODUCED TO PUPILS?

- All users are informed that network and Internet use will be monitored.
- E-safety forms part of the Computing Curriculum and the Anti-Bullying Policy.

- Pupils will be required to sign a Pupils' Acceptable Use Policy on starting Year Three, and will be taught the rules relating to e-safety in independent work at this time.

HOW WILL THE POLICY BE DISCUSSED WITH STAFF?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

HOW WILL PARENTS SUPPORT BE ENLISTED?

- Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.
- We will hold annual Parents' e-safety events to allow discussion of up-to-date e-safety issues.

Appendix One - E-Safety Contacts and References.

E SAFETY CONTACTS AND REFERENCES

Becta *www.becta.org.uk/safeguarding*

Child Exploitation & Online Protection Centre *www.ceop.gov.uk*

Childline *www.childline.org.uk*

Childnet *www.childnet.com*

Click Clever Click Safe Campaign *http://clickcleverclicksafe.direct.gov.uk*

Cybermentors *www.cybermentors.org.uk*

Digizen *www.digizen.org.uk*

Internet Watch Foundation *www.iwf.org.uk*

Kidsmart *www.kidsmart.org.uk*

Teach Today *http://en.teachtoday.eu*

Think U Know website *www.thinkuknow.co.uk*

Virtual Global Taskforce — Report Abuse *www.virtualglobaltaskforce.co*

Appendix Two School Internet Rules- Pupil

Acceptable Use Policy- Staff

SCHOOL INTERNET RULES

- I will not deliberately use the computers to try and find any material that might upset me, or other children or adults.
- If I am found using the Internet to find unsuitable material I will be banned from using the Internet for a period of time and my parents / guardians will be told.
- I will stay **safe** by never telling anyone my real name, address, phone number or school when I am using the Internet.
- I will never **meet**, or arrange to **meet**, anyone I meet on the Internet or by email or messaging.
- I will only send or **accept** an email or message with permission and when there is an adult with me.
- I will only send emails to an address I know and I will always use polite language.
- I will only use the Internet for schoolwork, with adult permission and when an adult is with me.
- I know that some information might not be **reliable** and I will check with an adult if I am unsure.
- I will not copy other people's work without **telling** them and getting their permission first.
- If I find anything that upsets me on the Internet, I will turn off the monitor straight away and **tell** an adult.
- I know that teachers will be able to **tell** what I have been looking at on the Internet by checking the history list of websites.
- I will not alter, change or delete any of the settings and files on the computers unless I have permission. I will **tell** an adult if I do this by accident.

E-SAFETY POLICY AGREEMENT

I have read, understand and agree wholeheartedly with all of the above information. I will ensure that I work with the other members of the ICT Team to ensure this E-Safety Policy is implemented across St John's CE Academy

Signed ……Name Signature Date ……..

ICT Subject Leader _____ _____ _____

Head Teacher _____ _____ _____

Acceptable Use Policy : Staff

1. Do not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.

2. Do not give personal addresses, telephone / fax numbers of

(i) any adult working at the school,
(ii) any students at the school.

Use of names of students, or photographs of students will require written permission from parents. This also applies to any work done by students, related to their education at St Johns Primary School. This is recorded on the Parental Agreement Form

3. Do not download, use or upload any material and use material which is copyright. Always seek permission from the owner, before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material

4. Under no circumstances should you view, upload or download and material which is likely to be unsuitable for children. This applies to any material of a violent, dangerous or inappropriate sexual content.

5. Always respect the privacy of files of other users. Do not enter the file areas of other staff without their express permission.

6. Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do not state anything which could be interpreted as libel.

7. Arrange for suitable monitoring of students in your class, or those students who you have given permission to use the Internet facilities.

8. Ensure that all students have followed the correct procedures:

(i) before starting the session,
(ii) during each session , and
(iii) on completion of the session.

9. Report any incident which breaches the Acceptable Rules Policy immediately to the headteacher or ICT coordinator. Do not attempt to investigate the incident, do not alter the computer in any way, and do not turn it off.

10. Remember that personal use of social media outside of work can reflect on your professionalism at school. Think carefully about what your posts say about you!

E-SAFETY POLICY AGREEMENT

I have read, understand and agree wholeheartedly with all of the above information. I will ensure that I work with the other members of the ICT Team to ensure this E-Safety Policy is implemented across St John's CE Academy

Signed ……Name Signature Date ……..

ICT Subject Leader _____ _____ _____

Head Teacher _____ _____ _____

Appendix Three E-safety Strands of the Curriculum by Year Group

Foundation	Year One	Year Two	Year Three	Year Four	Year Five	Year Six
★ I can ask an adult when I want to use the Internet. ★ I can tell an adult when something worrying or unexpected happens while I am using the Internet. ★ I can be kind to my friends. ★ I can talk about the amount of time I spend using a computer / tablet / game device. ★ I am careful with technology devices.	★ I can keep my password private. ★ I can tell you what personal information is. ★ I can tell an adult when I see something unexpected or worrying online. ★ I can talk about why it's important to be kind and polite. ★ I can recognise an age appropriate website. ★ I can agree and follow sensible e-Safety rules.	★ I can explain why I need to keep my password and personal information private. ★ I can describe the things that happen online that I must tell an adult about. ★ I can talk about why I should go online for a short amount of time. ★ I can talk about why it is important to be kind and polite online and in real life. ★ I know that not everyone is who they say they are on the Internet.	★ I can talk about what makes a secure password and why they are important. ★ I can protect my personal information when I do different things online. ★ I can use the safety features of websites as well as reporting concerns to an adult. ★ I can recognise websites and games appropriate for my age. ★ I can make good choices about how long I spend online. ★ I ask an adult before downloading files and games from the Internet. ★ I can post positive comments online.	★ I choose a secure password and an appropriate screen name when I am using a website. ★ I can talk about the ways I can protect myself and my friends from harm online. ★ I use the safety features of websites as well as reporting concerns to an adult. ★ I know that anything I share online can be seen by others. ★ I choose websites, apps and games that are appropriate for my age. ★ I can help my friends make good choices about the time they spend online. ★ I can talk about why I need to ask a trusted adult before downloading files and games from the Internet. ★ I comment positively and respectfully online and through text messages.	★ I can choose a secure password and screen name. ★ I protect my password and other personal information. ★ I can explain why I need to protect myself and my friends and the best ways to do this, including reporting concerns to an adult. ★ I know that anything I post online can be seen, used and may affect others. ★ I can talk about the dangers of spending too long online or playing a game. ★ I can explain the importance of communicating kindly and respectfully. ★ I can discuss the importance of choosing an age-appropriate website, app or game. ★ I can explain why I need to protect my computer or device from harm.	★ I protect my password and other personal information. ★ I can explain the consequences of sharing too much about myself online. ★ I support my friends to protect themselves and make good choices online, including reporting concerns to an adult. ★ I can explain the consequences of spending too much time online or on a game. ★ I can explain the consequences to myself and others of not communicating kindly and respectfully. ★ I protect my computer or device from harm on the Internet.

Appendix Four- eSafety Incident Report Form

St John's Church of England Academy

eSafety Incident Report Form

Date of Incident:

Names of persons involved:

Details of incident:

Internet sites involved:

Please attach any printouts of messages sent, including header information where possible.

Action taken: