St. John's
C OF E PRIMARY ACADEMY
BELIEVE TO ACHIEVE

St John’s C of E Primary Academy

E-Safety Policy

Author:	**D. Carlile**
Date of issue:	**May 2017**
Review date:	**May 2018**

Key Personnel

Principal: Sarah Cockshott

Chair of Governors: Fr Roger Gilbert

St John's Primary Academy

ICT E-Safety Policy

Introduction

This online safety policy is to ensure everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks whilst continuing to benefit from the opportunities that are available from using the Internet and new technologies. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put users at risk; these risks can be categorised into three main areas:

- **Content: being exposed to illegal, inappropriate or harmful material.**

- **Contact: being subjected to harmful online interaction with other users.**

- **Conduct: personal online behaviour that increases the likelihood of, or causes, harm.**

We aim always to keep our pupils safe whilst encouraging them to meet their full potential.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, work placement students, visitors), who have access to and are users of school ICT systems, both in and out of school.

The school will identify within this policy how incidents will be managed and will, where appropriate, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Principal believes it contains any illegal content or material that could be used to bully or harass others.

Good Habits

Online Safety depends on effective practice at a number of levels:

- responsible ICT use by all staff and pupils, encouraged by education and made explicit through published policies;

- sound implementation of online safety policy in both administration and curriculum, including secure school network design and use;

- safe and secure broadband from the local Grid for Learning, including the effective management of content filtering;

- national education network standards and specifications;

- pupil data to be kept within the secure network. To enable staff to work from home, data should only be taken from the building electronically, using encrypted software (mainly through the use of an encrypted flash drive).

School Online Safety Policy

As the roles overlap, the Principal is both the online safety co-ordinator and the designated child protection officer.

Our online safety policy has been written by the school, building on government guidance. It has been agreed by the senior management team and approved by governors.

The online safety policy will be reviewed annually.

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 administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element of 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How Internet Use Benefits Education

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- education and cultural exchanges between pupils world-wide;
- 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 support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with CYPS (Child and Young People Services) and the Department for Education;
- access to learning wherever and whenever convenient.

How Internet Use Enhances Learning

Internet use enhances learning by:

- ensuring access is designed expressly for pupil use and includes filtering appropriate to the age of pupils;
- teaching pupils what is and what is not acceptable and giving clear objectives for Internet use;

- planning Internet access to enrich and extend learning activities;
- guiding pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity;
- educating pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

Parents will be informed that pupils will be provided with supervised Internet access.

Staff will be made aware of the online safety policy and Internet usage through the induction process.

World Wide Web

If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported using the pro-forma on staff share and passed onto the online safety co-ordinator or network manager.

School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

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

Email

Pupils may only use approved email accounts on the school's internal system.

Pupils must immediately tell a teacher if they receive offensive email.

Pupils must not reveal personal details relating to themselves or others in email communication or arrange to meet anyone without specific permission.

Whole class or group email addresses should be used in school.

Access in school to external personal email may not be used by pupils.

The forwarding of chain letters is not permitted.

Social Networking

The school has blocked access to social networking sites and newsgroups unless a specific use is approved.

Please be advised of minimum age restrictions on social media (this list is not exhaustive):

Twitter	13
Facebook	13
Instagram	13
Pinterest	13

Tumblr 13

Reddit 13

Snapchat 13

LinkedIn 14

WhatsApp 16

Vine 17

YouTube 18 (although children aged 13-17 can signup with parent's permission)

The pupils will be advised to never give out personal details of any kind which may identify them or their location. The pupils should be advised not to place personal photos on any social network space.

The pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the CYPS and the Internet service provider (TrustNet) to ensure filtering systems are as effective as possible.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Pupils are not allowed to bring mobile phones to school. Any exceptions to this are by arrangement with the Principal /office and parents. Any phone brought to school inadvertently must be switched off and handed to the Principal /office for safekeeping.

Published Content and the School Website

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

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 or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Work can only be published with the permission of the pupil and parents.

Information System Security

School ICT systems' capacity and security will be reviewed regularly.

Virus protection will be installed and updated regularly.

Security strategies will be discussed with the local advisors.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

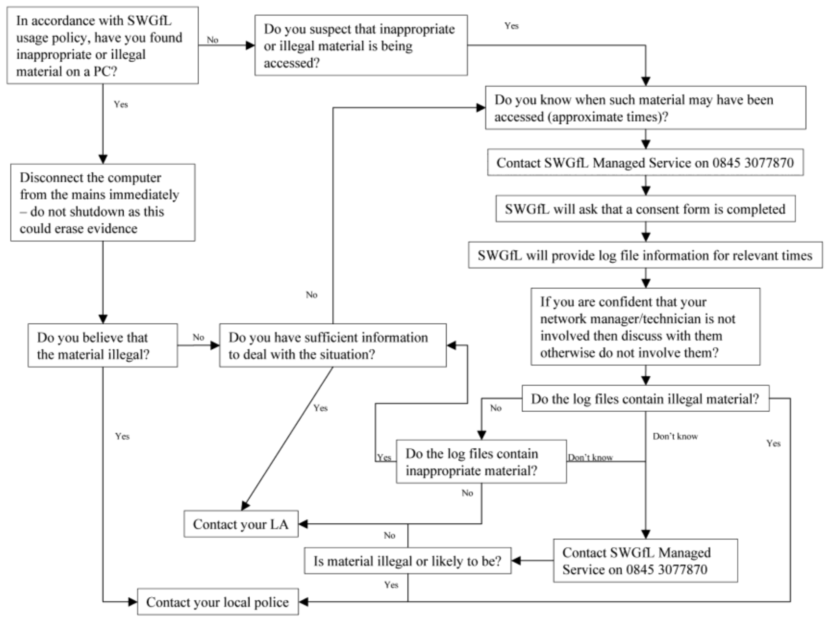
Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the local council can accept liability for the material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

Handling Online Safety Incidents and Complaints

Refer to the flowchart for responding to online safety incidents.


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
Yes
No
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

SWGfL = South West Grid for Learning

Complaints of internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Principal.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Discussions will be held with the Police Youth Crime Reduction Officer or Community Police Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

Rules for Internet access will be posted in all networked rooms.

Pupils will be informed that Internet use will be monitored.

They will also sign an agreement in collaboration with their parents confirming they have read and understood the policy.

Staff:

All staff will be given the school online safety policy and its importance explained. They will also sign an agreement confirming they have read and understood the policy.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents:

Parents' attention will be drawn to the school online safety policy in newsletters, the school prospectus and on the school website. A hard copy will be available in the main office.

They will also sign an agreement in collaboration with their children confirming they have read and understood the policy.

ACCEPTABLE INTERNET USE STATEMENT FOR ALL SCHOOL STAFF

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an Internet Access Policy drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access should only be made via the authorised account and password that should not be made available to any other person.

- The security of the ICT system must not be compromised whether owned by the school, by or any other organisation or individual.

- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.

- Users are responsible for all e-mail sent and for contacts made that may result in email being received.

- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.

- Posting anonymous messages and forwarding chain letters is forbidden.

- Copyright of materials and intellectual property rights must be respected. • All staff should take great care in using social networking sites so that their own or their colleagues professionalism and privacy are not compromised.

- All Internet use should be appropriate to staff professional activity or to student's education. However please note that:-
    - The school's ICT system may be used for private purposes following guidelines established by the school.
    - Use for personal financial gain, gambling, political purposes or advertising is forbidden.
    - Closed discussion groups can be useful but the use of public chat rooms and social networking sites is not allowed on school IT equipment on the school premises.

Members of staff are reminded that they should not deliberately seek out inappropriate / offensive materials on the Internet and that they are subject to the LEA's recommended disciplinary procedures should they do so. Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

Full name ____________________ Signed ____________________ Date ______________

Letter to parents

Dear Parents

Responsible Use of the Internet

As part of pupils' curriculum enhancement and the development of ICT skills, St John's Primary Academy is providing supervised access to the Internet including e-mail.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet access provider, TrustNet, operates a filtering system that restricts access to inappropriate materials. This may not be the case at home. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, St John's Primary Academy cannot be held responsible for the nature or content of materials accessed through the Internet. The Council will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

I enclose a copy of the Rules for Responsible Internet Use that we operate at St John's Primary Academy School. Could you and your child please sign and return to school the agreement below to help us operate our safe internet usage policy.

Should you wish to discuss any aspect of Internet use at school please telephone me to arrange an appointment.

Yours sincerely,

Sarah Cockshott

Principal

Permission for Internet Access

Parent/carer's permission

I give permission for access to the Internet on the terms set out in the above letter.

Signed ____________________ Print name______________________ Date ______________

Pupil’s agreement

I agree to follow the Rules for Responsible Internet Use.

Signed ____________________ Print name______________________ Date _____________

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will use only my own login and password, which I will keep secret. (Where I create my own username, it will be appropriate to me and my school.)

- I will not access other people's files.

- I will use the computers only for schoolwork and homework.

- I will not bring USB memory pens into school without permission.

- I will ask permission from a member of staff before using the Internet;

- I will only e-mail people I know, or my teacher has approved;

- The messages I send will be polite and sensible;

- I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;

- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive a message I do not like;

- **I understand that the school can check my computer files and the Internet sites I visit.**

Online Safety Suggestions for Parents of Young Children

This document will give you some hints and tips to keep your children safe on the internet, when using computers, tablets and phones, and when accessing social media. Young children are increasingly digitally literate, and as adults, we need to know what they are up to and teach them how to keep safe online.

Social media:

Technically, children under the age of 13 shouldn't be building profiles on Facebook, Instagram and Snapchat etc. This is difficult, as many of their friends may already have profiles. Some sites such as YouTube, allow for children aged 13-17 to have profiles under their parent's consent. Twitter's terms of use are a little more confusing, and imply that children under 13 can have a profile with their parent's consent. When your children are old enough to access social media, take time to sit with them and go through privacy settings, explaining who can see what they publish.

Passwords:

Though you need to be teaching your children about password safety, and encouraging them not to share passwords with their friends, you also need to let them know that you can and will have access to their equipment and that you need to have access to their password, even if you don't memorise it. This will help them if they lock themselves out of their equipment by forgetting their password, and also means that you can go in and oversee their online behaviours, with their permission. Teaching them how to create a strong password is a good idea – starting with mixing numbers and letters with very young children. Take time to explain your reasons for needing to know their password, and why they shouldn't share it with anyone else.

Messaging and group chat:

This can be a tricky area to police, as by its very nature, it is hidden from public view. Make sure that you check in with your child regularly about their group chats, who is taking part in them, and make sure that they are only talking to people that they know in real life. Ask them to show you some of the conversations so that you can get a feel for what's going on in the chats. Keeping an open dialogue will help to maintain the trust between you and your children, and will ensure that your child will feel that they can come and talk to you if something is worrying them online.

Gaming:

Lots of children enjoy gaming on their video consoles and on the internet. Open and closed groups can easily be set up by children, and you need to know what is going on in their online play, in the same way as you do in their face-to-face relationships. Sit with them whilst they are engaged in their games, and ask them about what is happening. Who are they talking to? What are they playing together? Build up an interest in their game playing, and again, you will open that dialogue to engage with your child if they feel things are worrying them.

The most important thing you can do, is talk to your child. Engage in their interests and find out what they are up to. Talk the talk, and they will feel confident to talk to you if things are troubling them online.

Top Tips

Online Internet Safety for Staff in Schools

This document will give you some hints and tips to keep YOURSELF safe on the Internet, and when using social media. Staff in schools are particularly exposed and need to consider their own actions in terms of compliance with school policy, as well as protecting their privacy.

Passwords

Make it a habit to change your password every 6 months, or more if you feel that it may have been compromised. Good password protocol is usually triggered when setting a password and gives you a 'strength rating' (weak, moderate, strong etc.) and will guide you to set a stronger password. If not, always use a variety of characters / numbers / uppercase and lowercase letters to create a strong password. Don't use birthdays or family names, names of pets or recurring number groups. And most importantly, don't use the same password for all of your internet activity! Mix it up. Keep yourself safe.

Social Media

Everyone's on Facebook, aren't they? Yes. Everyone. Keep your school activities off Facebook and never post pictures of a staff night out with your colleagues. Keep your privacy settings locked down and never accept friend requests from children in your school. With Twitter, you are asked to create a public or private account at the start – make a decision there and then. If it's public, everyone can see what you write, even if they don't follow you. So be professional, or lock it down. Same with Instagram and blogging. They are great ways to connect with your friends, but sometimes it's more than just your friends who are viewing your holiday snaps.