



ONLINE SAFETY POLICY

Contents

School Online Safety Policy	2
Why is Internet use important?	2
How does Internet use benefit education?	3
How can Internet use enhance learning?	3
Authorised Internet Access	3
World Wide Web	Error! Bookmark not defined.
Email	3
Social Networking	4
Filtering	4
Video Conferencing	5
Managing Emerging Technologies	5
Published Content and the School Web Site	6
Publishing Pupils' Images and Work	6
Information System Security	6
Protecting Personal Data	6
Assessing Risks	6
Handling Online Safety Complaints	6
Communication of Policy	7
Pupils	7
Staff	7
Parents	7

Appendices

- Flowchart for Responding to Online Safety incidents
- Pupil Acceptable Use Policy
- Online Safety Rules
- Online Safety Rules - Parent Consent
- [Staff Information Systems Code of Conduct](#)
- Online Safety Audit Tool

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users)

Research has proven that the use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings the element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's Online Safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Curriculum and Data Protection.

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 Lancashire Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

School Online Safety Policy

The school's online safety coordinator is Miss Hartley - the Designated Senior Leader for Child Protection.

Our online safety Policy has been written by the school, building on advice from BECTA and guidance from the local authority and agreed by governors.

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 in 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 does Internet Use Benefit 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;
- educational 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 the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be 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.
- Staff should guide pupils in on-line activities that will support 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.
- Use of child friendly internet access can be used using kiddle.co.uk.

Authorised Internet Access

- Parents are informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access upon entering in Reception or as a new pupil.

Internet

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the Online Safety coordinator or network manager (Mrs Swanney and the Headteacher).
- 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 e-mail accounts on the school Purple Mash system which is set up for the teacher to review prior to sending.
- Pupils can report offensive e-mails which teachers are able to review, explaining to a pupil this has been rejected.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations 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 is not permitted.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils should be made aware of age rating of social media networks.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- 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 Local Authority, BECTA and the Internet Service Provider to ensure filtering systems are as effective as possible. The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that our school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

A summary of the service provided by BT Lancashire Services (Lightspeed Systems) is displayed below:

About the Service



What is it?

Our Internet Filtering (Lightspeed Systems) service is a centrally hosted web filtering provision enabling safe internet access for schools.

Why do I need it?

It provides you with the flexibility to locally manage and control access to websites. The service provides the following functionality for schools:

- Education focussed web filtering.
- Ability to filter based on IP address ranges or by using an external directory such as your School's active directory domain.
- Local control to allow your School to manage which websites it wishes to allow or block.

What are the benefits?

Schools have the ability to implement granular filtering based on individual classroom or user needs, removing dependence on BT Lancashire Services to block / unblock individual websites for individual school requests.

Schools do not require any filtering equipment to be installed in school with this service

Video Conferencing

Video conferencing is not currently used at St Anne's but should we consider using it in the future, the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- A permissions letter will be made available for parents/carers to sign giving permission for their child/children to participate in video and photographs. Children will not be appearing 'live' on the Internet through a video conferencing link.
- Approval by the Headteacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/person(s) taking part.
- Pupils using video conferencing equipment should be supervised **at all times**.
- All staff supervising the video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'stop' or 'hang up' the call.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.
- Recordings will not be repurposed in any other form or media than the purpose originally agreed.

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.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

- Children's mobile phones are not allowed in St Anne's unless by permission of the Headteacher and left in her office.

Published Content and the School Web Site

- The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupil's personal information will not be published.
- The Head teacher has overall editorial responsibility and ensures 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 Web site 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 Web site.
- 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 Authority.

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 LEA can accept liability for the material accessed, or any consequences of Internet access.
- The school will monitor 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 Complaints

- 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.
- 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 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.

Staff

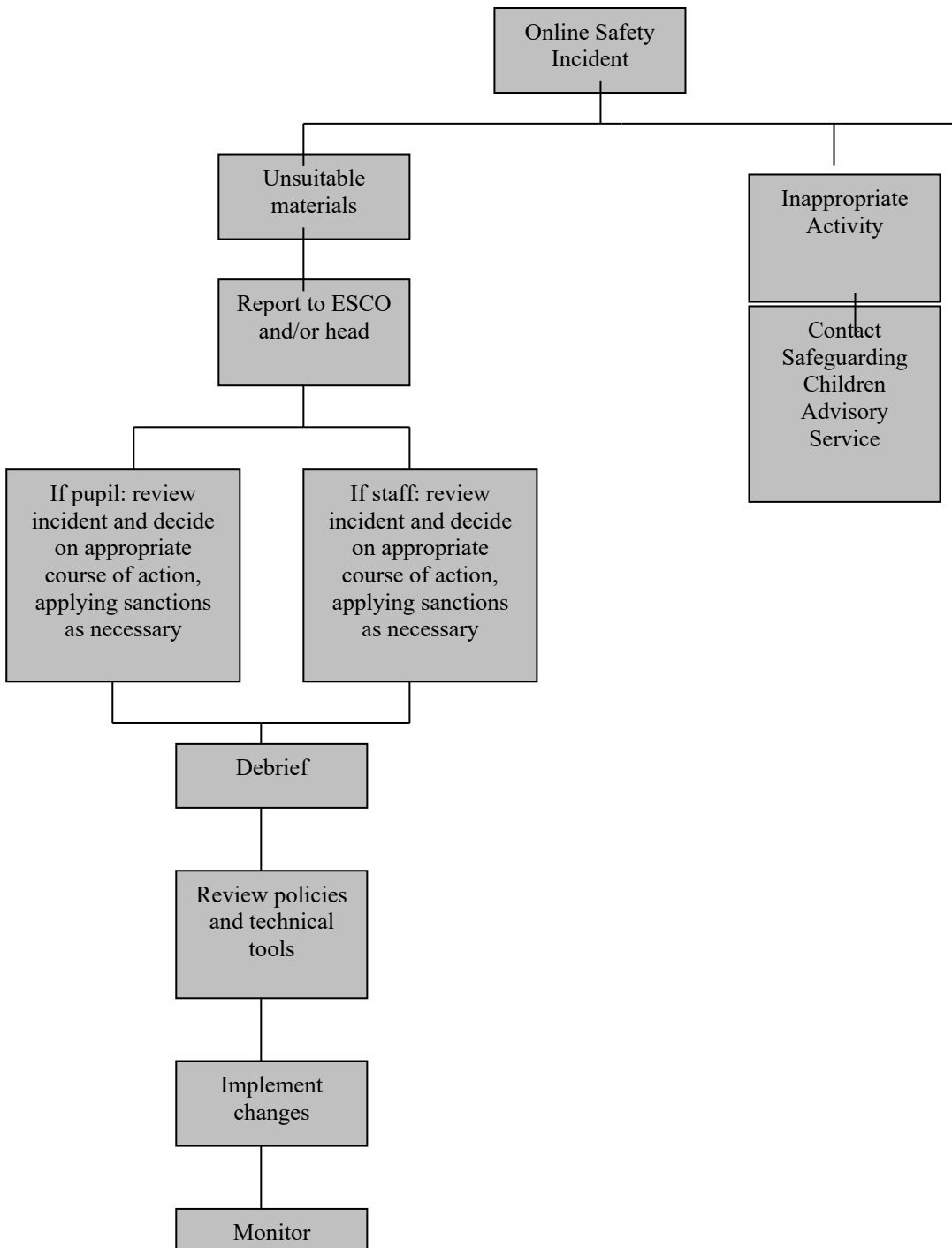
- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.

Appendix A

Flowchart for responding to Online Safety incidents in school



Adapted from BECTA – Online Safety 2005

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet



We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.

We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.



Key Stage 2

Think then Click

Online Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage that we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone that we don't know.
- We do not use Internet chat rooms.

Online Safety Rules

These Online Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

St Anne's CE Primary School



Online Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school Online Safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:

Date:

Please print name:

Please complete, sign and return to the school

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school Online Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: Capitals: Date:

Accepted for School

Online Safety Audit

This self-audit tool helps the Leadership Team assess whether the Online Safety basics are in place.

Has the school an Online Safety Policy that complies with the LEA guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The Online Safety Coordinator is:	
Has Online Safety training been provided for both pupils and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School Online Safety Rules?	Y/N
Have school Online Safety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	Y/N
Has the school filtering policy has been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N