



**St Bonaventure's Catholic Primary School
Egerton Road,
Bishopston
Bristol,
BS7 8HP**

E-Safety Policy 2017

Policy Owner	Headteacher
Governing Body Committee	MECP
Issue Date	14.10.15
Last Review Date	05.04.17
Next Review Date	Term 1 2018/19

This policy is available at
<http://www.st-bonaventures.bristol.sch.uk/>



Network Security

The school has a responsibility for ensuring that its capital investment is protected and secured, just as there are procedures for building security and safety.

All users will understand that no changes or modifications to the hardware, network wiring, or software configurations will be tolerated. Forbidden changes include introducing software and code from outside sources or connecting personal equipment (such as a PDA or laptop) to the network without agreement from the school. Only designated support personnel will perform these functions and all work will be logged.

Network traffic across the school local area network (LAN) cannot anyway be accessed outside the premises. Wireless LAN broadcasts may be monitored beyond the school boundary and encrypted transmission can be configured to prevent access.

The school has a security policy to control user permissions on the network. Network administrators understand the principles of file level security and the consequences of access. Users who have network administration rights must safeguard their access and understand their responsibilities.

A clear network backup and data archiving regime is defined and followed by the ICT leader and Technician. Responsibility for performing backup procedures and monitoring activity logs is clearly-defined and is managed at senior level.

Where Internet and wide area network (WAN) connectivity is involved, security measures such as network firewalls, audit trails and attack alerts are reviewed. These considerations will protect not only the school's LAN system but also beyond to the education and LEA WAN community.

All ICT equipment is recorded and security-marked. Safety testing and maintenance logs are kept. Hardware maintenance contracts include network components hubs, switches.

Internet

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

St Bonaventure's Primary School uses Bristol LA to deliver internet access to the school. This service provides:

- facility for multiple access;
- educational content (for example access to schools' web pages, projects, educational resources, professional discussion groups);
- filtering from the less desirable elements of the internet;
- filtering of junk mail;
- the ability to configure, for example, to limit access to news groups, chat rooms;
- availability of free web space;
- Outlook email addresses provided;
- fixed low cost.

The school will work in partnership with parents, Bristol County Council, DfE and the South West Grid for Learning ("SWGfL") to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (address) and content **must** be reported to the internet Service Provider on **0117**



9037999 (cyps.it.helpdesk@bristol.gov.uk) and recorded on the E-safety log that is monitored by the IT Leader and the IT Committee.

Pupils will learn appropriate internet use and be given clear objectives for internet use. Sophos virus protection software is installed on all school systems. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. The use of on-line resources is always supervised.

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. Neither the school nor Bristol County Council can 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 monitored.

Teachers will be familiar with the Pupils' "Code of Practice" for use of the Internet and will sign the Teachers' "Code of Practice" before access to the Internet is provided. Parents will be informed that pupils will be provided with supervised internet access - Pupils and Parents/Carers will read and sign the Code of Practice for Pupils before a password is issued to pupils. *All users should adhere to the Code of Practice.*

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.

The law is quite clear on computer pornography. The Obscene Publications Act 1959 and 1964 makes it an offence to publish an obscene article (whether for gain or not) or to have an obscene article for publication or gain (publication includes distribution, circulating, selling, hiring, giving or lending, showing, playing or projecting). Teachers and other adults have a responsibility to protect the children from viewing unsuitable materials. St Bonaventure's School will make clear the disciplinary actions which will be taken in the event of teachers using the Internet inappropriately as set out in the Disciplinary Procedure.

If pupils either deliberately or accidentally access or download unsuitable materials staff/adults will follow the following procedure:

- the screen will be turned off;
- any printed materials or disks will be confiscated;
- the pupil's access to the Internet will be suspended until further investigation;
- the Headteacher will be informed;
- the E-safety log will be completed.

The ICT leader and Technician will audit user areas on networks to reveal unexpectedly large graphic files with, for example, .GIF or .JPG extensions or with names with series of meaningless letters and numbers. These can be indicators of downloading of inappropriate files.

All Internet activity should be appropriate to staff professional activity or pupils' education (however the school wishes to encourage individuals to use the computer in a constructive way and occasional personal use is permitted at the discretion of the school).



On the school's own website, the point of contact will be the school address, school email and telephone/fax number. Staff or pupils' home information will not be published. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the pupils to be identified. Should parents not give permission for their children's photos to be published the school will respect this decision and ensure they do not place such photos on the School website or any other publication. Any identified vulnerable children who have safeguarding measures in place surrounding exemption of sharing digital images of themselves will not have their images placed in the public domain.

Rules for internet access will be posted in all rooms where computers are used. All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School internet Policy, and its importance explained. All staff/pupils/adults must accept and sign the relevant 'Code of Practice' before using any internet resource in school.

The school follows the SMART code of practice (safe, meeting, accepting, reliable, tell). The rules are explained to the children and displayed where computers are used.

Electronic Email, Chat and Communication

Appropriate language will be used for all on-line communications. Electronic communication will not be used to create, use, transmit or encourage material which is:

- pornographic, inappropriate or unsuitable;
- illegal, obscene or libelous;
- offensive or annoying;
- defamatory;
- violates another person's privacy.

Electronic communication will not be used for gambling, advertising or soliciting for personal gain or profit.

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

Posting anonymous messages and forwarding chain letters is forbidden.

Users will not sign up to any information services, i.e. services, which send you regular information via email or other electronic means unless this is directly related to school activities.

Users will not transmit any material in violation of any British laws. These include the Data Protection Act, Computer Misuse Act and Design Copyright and Patents Act. This includes, but is not limited to, copyright material, threatening or obscene material, material protected by trade secret or any sensitive personal data, confidential, classified or proprietary information.

Users will not use email for product advertisement, commercial activities or political campaigning, unless authorised to do so by the school. The school's resources should not be wasted by indiscriminate use of email. For example, only send an email to those staff or pupils directly interested in a topic. The school should not be committed to purchasing or acquiring goods without proper authorisation. Users will log off properly from networks after use to ensure that other users do not have unauthorised access.

Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.



Students/pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific ICT lessons dedicated to e-safety. The use of online chat is not permitted in school, other than as part of its online learning environment.

Cyber-bullying

St Bonaventure's Primary School takes issues of Cyber-bullying (occurring both on and off of the school site) very seriously.

Cyber bullying is the use of ICT (usually a mobile phone and or the internet) to abuse another person.

It can take place anywhere and involve many people.

Anybody can be targeted including pupils and school staff.

It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorized publication of private information or images etc.

We work closely with families to help them ensure that their children use new technologies safely and responsibly. We provide an age-related, comprehensive curriculum for e-safety (including cyber-bullying in all forms) that enables pupils to become safe and responsible users. This comes from the acceptable use strand of our scheme of work, as well as through whole-school and key stage assemblies, and additional class-work (for example during anti-bullying week). Incidences of cyber-bullying are logged and dealt with according to the procedures for dealing with any other type of bullying incident. Children are expected to follow the rules set out in the Acceptable Use document when using technologies in school. Staff training on cyber-bullying is regularly updated through INSET, staff meetings and emailed information bulletins.

This policy should be read in conjunction with the Internet Code of Practice for Pupils and Teachers and Adults, Disciplinary Procedure, Behaviour Policy and Anti-bullying Policy.



Internet Code of Practice for KS2 Pupils

We use computers and internet connection for learning and research.

These rules will help us to be fair to others and keep everyone safe.

- I will only use the internet when supervised by a teacher or adult.
- At the start of the school day I will hand in my mobile phone to the school office, and collect it at the end of the school day. I will not bring my phone into the classroom and I will not keep it in my bag.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name without permission, or send a picture of myself. I will never arrange to meet anyone in person.
- I will never give any passwords to anyone, even my best friend, and I will log off when I have finished using the computer.
- I will never answer unpleasant, suggestive or bullying emails or messages and I will always report it to a teacher or parent.
- I will not look for bad language or inappropriate images and I will report bad language or inappropriate images to a teacher or parent if I come across them accidentally. I know that my teacher can check the websites I have visited!
- I will always be myself and will not pretend to be anyone or anything I am not. I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I understand that I can only use websites for my work in school and that I will not be allowed to use the Internet if I look at unsuitable material on purpose.
- I may not download **any** software from the Internet. I know that information on the Internet may not always be reliable and may need checking. I know that some web sites may be sponsored by advertisers.
- I will not use email to send or encourage material which is illegal, offensive or annoying or invades another person's privacy.



I have read the Internet Code of Practice for Pupils document and I agree to support the school's policy.

Signed _____

Date _____

Name _____

Class _____



Internet Code of Practice for KS1 Pupils

We use computers and the internet for learning.

These rules will help us to be fair to others. They will help keep everyone safe.

- I will only use the internet when I am near a teacher or adult.
- I will never tell anyone I talk to on the internet where I live or what my school is called, or send a picture of myself, unless a teacher or adult I know says it is okay. I will never say I will meet anyone in real life.
- I will never give any passwords to anyone, even my best friend, and I will log off when I have finished using the computer.
- I will never answer unkind messages and I will always tell a teacher or parent about it.
- I will not look for bad words or pictures and I tell a teacher or parent if I see them by accident. I know that my teacher can check the websites I have seen!
- I will always be myself. I will not pretend to be anyone or anything I am not.
- I know I can only use websites for my work in school. I will not be allowed to use the internet if I look at bad things on purpose.
- I will not use the internet to send things which are illegal, mean or annoying. I will not say things on the internet about other people unless they say it is okay.



I have read these rules. I agree to follow these rules.

Signed _____

Date _____

Name _____

Class _____





Internet Code of Practice for Teachers and Adults

Teachers/adults should be familiar with the school's E-Safety Policy and the St Bonaventure's responsible internet use guidelines for pupils.

Teachers should closely monitor and scrutinise what their pupils are accessing on the internet, including checking the history of pages. Computer monitor screens should be readily visible to the teacher, so they can monitor what the pupils are accessing.

Pupils should be given clear guidelines for the content of email messages and for sending and receiving procedures.

Use of the iPads should be supervised by a teacher or adult. A list of which pupil uses which iPad shall be maintained and where possible adhered to by the teacher.

Pupils should have a clearly defined focus for using the Internet and email. It is recommended that pupils do not use open forums such as newsgroups or chat rooms. Pupils should be taught skills and techniques to enable efficient and effective use of the Internet.

If offensive materials are found, the monitor should be switched off, any printed materials or disks should be confiscated and offensive URLs should be given to the ICT leader / Technician who will report it to Bristol CYPS. The incident should be reported to the Headteacher.

Virus protection has been provided by the school as viruses can be downloaded accidentally from the Internet. Pupils bringing work from home on data keys could also infect the computer - some viruses will format your hard drive!

Disciplinary action may be taken if the Internet is used inappropriately, for example, by accessing pornographic, racist or offensive material or for personal financial gain, posting photos of children, gambling, political purposes or advertising.

Software should not be downloaded from the Internet (including screen savers, games, video clips, audio clips, *.exe files) or installed by anyone other than the ICT Technician unless agreed with the ICT leader in advance.

I have read the *Responsible Internet Use* document for pupils and teachers and I am familiar with the school's policy on the use of the Internet, e-mail, the creation of web sites and network security.

I understand the insurance and care implications of any equipment loaned from school and agree to abide by the St Bonaventure's Teacher's Code of Practice.

✂

I have read the E-Safety Policy and Code of Practice for Pupils. I agree to support the school's policy.

Signed _____

Date _____

Name _____