



Bishop Bridgeman Church of England Primary School

e-Safety Policy

This policy outlines our purpose in providing e-mail and access to the Internet at Bishop Bridgeman and explains how the school is seeking to avoid the potential problems that unrestricted Internet access could give rise to.

INTERNET ACCESS IN SCHOOL

Providing access to the Internet in school will raise educational standards and support the professional work of staff.

Teachers will have access to the Internet offering educational resources, news and current events they will also be able to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LEA and DCSF. The Internet is being used to enhance the school's management information and business administration systems.

Pupils will have access to the Internet offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others world-wide.

All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the Internet will be provided with the School Internet Access Policy and will have its importance explained to them.

Parents will be drawn to the Policy by letter in our school prospectus and online within the ESafety section of the schools' Learning Platform.

USING E-MAIL

All staff are strongly advised **NOT** to use or share their personal email account for school and therefore are issued with their own professional email which they will use appropriately to communicate with colleagues and schools external services.

Pupils will learn how to use an e-mail application

- Once they have been taught the Rules of Responsible Internet Use and agreed their Acceptable User Policy on the Learning Platform;
- Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
- Pupils will not be permitted to use e-mail at school to arrange to meet someone outside school hours.

INTERNET ACCESS AND HOME/SCHOOL LINKS

Parents will be informed in our school prospectus that pupils are provided with supervised Internet access as part of their lessons. We will keep parents in touch with future ICT developments by newsletters and the Learning Platform.

ESafety will be taught to all pupils from year 1 and will be readdressed every year. Sessions will be taught using age appropriate resources and cover the following areas: Email, SMS Messaging, Social Networking and Cyber Bullying. All children within these sessions will have the opportunity to agree to their own Acceptable Users Policy.

If a reported incident arises outside of school, staff will log the event with the ICT Co-ordinator, a letter will be sent home to inform parents and a discussion to take place with all parties.

SOCIAL NETWORKING

Online social networking and interactive services can provide extensive benefits to their users. However while staff and volunteers will want to make the most of these services, this document aims to ensure they understand the importance of protecting themselves, their online identities and their reputations. It is vital that staff / Governors / volunteers are aware of the importance of keeping private and professional information separate. Irresponsible use of new technologies can affect your reputation, your self-esteem, your health and, in some cases, your career progression.

Social networking sites include:

- Facebook
- Bebo
- Friends Reunited
- LinkedIn
- MySpace

- **Twitter Security Settings** It is vital that when you register to become a user of a social networking site, you ensure that you access the 'settings' page and set these to their highest possible level. This will ensure that only those people who you authorise to see your information will be able to see it, however remember that friends may respond to your comments, or post comments on your photographs which their friends are then able to see, and so on.

- **Friend Requests – Sending and Receiving**

- Under no circumstances must staff / Governors / volunteers accept friend requests from children / young people, nor should they make such requests. Should a young person attempt to contact you in this way, you should make this known to your manager immediately.

- **Remote access to social networking sites**

- Many staff / Governors / volunteers and young people now have the facility to access their social networking information 'on the move' and can keep it updated at all times via mobile phones, I-Pads etc. It is vital that these items are password protected to the highest level to avoid unauthorised access/use.

Social Networking Dos and Don'ts

Do

- Think about who you want to see your personal information
- Read the privacy settings information carefully
- Set your profile to 'private' / the highest security setting
- Review your 'friends' list regularly to ensure you still want them to know your personal details

- Think very carefully about what you share with friends, even if your information is 'private' as this may appear on your 'friends' page

- Protect your password and never share it with anyone else
- Only communicate with pupils via official school systems
- Be careful about the kind of information (including images) you share about yourself and how you manage your online reputation. Other people can pass on or change your information and you might not be able to stop them or delete it afterwards.
- Guard your online reputation
- Use a strong password – numbers as well as letters, upper and lower case, and never let anyone else have it

Don't

- Share information that shows you or your friends in a compromising situation
- Post content that may be seen as racist, homophobic, bullying or threatening
- Bring the school into disrepute by posting derogatory comments about your work/employer
- Use personal equipment, i.e. mobile phones or cameras to take photographs of children and young people
- Give any personal details, including your mobile number, to a young person.

USING INFORMATION FROM THE INTERNET

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly audited/edited and most of it is copyright.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true;
- When copying materials from the Web, pupils will be taught to observe copyright;
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed. If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly and on a number of levels
- Staff will log the event with the ICT Co-ordinator;
- A letter will be sent home to inform parents;
- Discussion to take place with all parties. Serious incidents within school will be referred to the Child Protection Officer in consultation with Principal and the pupil's class teacher. Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet by failing to follow the rules they have been taught and rules set

within the acceptable users' policy; then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers and access to the Internet may be denied for a period.

MAINTAINING THE SECURITY AND SAFETY OF THE SCHOOL NETWORK

- We are aware that connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons. As part of the ICT SLA agreement the school receives regular Sophos Anti-Virus software updates. However it is the schools duty to notify the LA if there is a possible virus risk.
- Our internet access is purchased from BOLTON LA, and the school has a “fileserver” which acts as the schools server, this provides a service designed for pupils including a “firewall” filtering system intended to prevent access to material inappropriate for children;
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils;
- Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;
- Staff to ensure that when searching the Internet for images all projectors and Smartboards to be turned off, enabling a wider use of images banks;
- If staff or pupils discover unsuitable sites the ICT co-ordinator will be informed. The URL (address) and content will be reported to the LA ICT support team;
- If it is thought that the material is illegal, after consultation with the LA ICT support team, the site will be referred to the Internet Watch Foundation and the police;
- Our Rules for Responsible Internet Use will be posted near computer systems;
- The Principal will ensure that the policy is implemented effectively. All staff have been trained how to backup their files –the school network, home shared files and their pen drives. Staff are aware of their responsibility of scanning all their external hard drive devices regularly and reporting any issues.
- It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor BOLTON LEA can accept liability for the material accessed, or any consequences thereof. A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Review Date: September 2017

Next review: September 2018