E-safety Policy
Stoke Bishop Primary School

1 INTRODUCTION

1.1 This policy has been developed to ensure that all adults at **Stoke Bishop Church of England Primary School** are working together to safeguard and promote the welfare of children and young people.

1.2 E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.3 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to address any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.4 The Head teacher, Deputy Head teacher, or, in their absence, the ICT Subject Leaders have the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.5 This policy complements and supports other relevant school policies, including the Staff Code of Conduct.

1.6 The purpose of internet use in school is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the school's management information and business administration systems.

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

1.8 A risk assessment will be carried out before children and young people are allowed to use new technology at Stoke Bishop School, e.g. Interactive Whiteboards.

2 ETHOS

2.1 It is the duty of the school to ensure that every child and young person in its care is safe. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its' everyday practice and procedures.

2.3 All staff have a responsibility to support e-safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policy.

2.6 Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

3 ROLES AND RESPONSIBILITIES

The Head teacher and ICT Subject leaders at **Stoke Bishop Church of England Primary School** will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal. That all staff are aware of the need to ensure that they consider, seriously, their own digital foot-print.
- The Computing Subject Leaders will receive appropriate on-going training, support and supervision and will work closely with the Designated Person for Safeguarding (head teacher).
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

The Governing Body of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school.
- Procedures are in place for dealing with breaches of E-safety and security and are in line with National procedures.
- All staff and volunteers have access to appropriate ICT training.

The Deputy Head teacher and the ICT Subject Leaders will:

- Act as a main point of contact, alongside the Safeguarding Leader with regards to breaches in e-safety and security.
- Liaise with the Safeguarding Leader as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received and signed a copy of the Schools E-safety and Internet Use Policy.
- Ensure that all staff and volunteers understand and are aware of the school's E-Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Regularly check files on the school's network.

4 TEACHING and LEARNING

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and pupils which benefits education by allowing access to worldwide educational resources including art galleries and museums, as well as enabling access to specialists in many fields for pupils and staff.

4.2 Access to the internet supports educational and cultural exchanges between students worldwide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local and National agencies.

4.4 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, Government initiatives.

4.5 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of pupils.

4.6 Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.7 Pupils will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information.

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

5 MANAGING INTERNET ACCESS

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Initially the pupils may be restricted to sites which have been reviewed and selected for content, through the teacher creating a file on the schools network for the children to access.

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening, using our SMART rules and Hector the dolphin.

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Subject Leaders, who will then contact the LA, for further guidance.

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

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

6 MANAGING E-MAIL

6.1 Personal e-mail or messaging between staff and pupils must not take place.

6.2 Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail.

6.3 Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.4 Staff must not use own personal e-mail accounts for specific school centred activities.

6.5 The forwarding of chain letters is not permitted.

6.6 Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

7 MANAGING WEBSITE CONTENT

7.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Parents must sign the parental consent form for photographs of pupils to be used. If a child does not have consent then the school is responsible for ensuring that no photographs of the child are used and that all staff are aware of this.

7.3 The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.

7.4 The Head teacher will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 The full names of pupils will not be used on the website, particularly in association with any photographs.

7.7 Parents/carers must sign the annual parental consent form for student's work to be used on the website.

7.8 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.9 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

8 SOCIAL NETWORKING

8.1 The school will make children aware of the risks and dangers of social networking sites. Parents will also be made aware that it is illegal to access particular social networking sites if children are of primary age.

8.2 Pupils will not access social networking sites e.g. Facebook or Twitter at school.

8.3 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.

8.4 Pupils will not be allowed to access public or unregulated chat rooms.

8.5 Pupils will only be allowed to use regulated educational chat environments and will be supervised.

8.6 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

9 MOBILE PHONES

9.1 Students are not permitted to bring mobile phones to school.

9.2 Staff are not permitted to take photographs with their own personal mobile phones. School digital equipment should be used to record any digital images.

10 FILTERING

10.1 The school will work in partnership with parents/carers, the Local Authority and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

10.2 If staff or pupils discover unsuitable sites, the URL **(address)** and content must be reported to the Computing Subject Leaders.

10.3 Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk).

10.4 Regular checks by the Computing Subject Leaders and the School's ICT support service will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.5 Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

10.6 If deemed appropriate, teachers will pre-select websites for children to use if around a potentially sensitive subject such as religion.

10.6.1 When accessing YouTube clips, teachers should check their suitability first before showing the pupils.

10.6.2 When accessing Google images, teachers should check their suitability first before showing the pupils.

10.6.3 When searching on the internet in general, teachers should check their suitability first before showing the pupils.

11 AUTHORISING INTERNET ACCESS

11.1 All staff must read and sign the school's E-Safety Policy before using any school ICT resources.

11.2 The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

11.3 The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access.

11.4 Staff will supervise access to the internet from the school site for all pupils.

12 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

12.1 It is not appropriate to use photographic or video technology in changing rooms or toilets.

12.2 Staff may use **school** photographic or video technology to capture or support school trips and appropriate curriculum activities.

12.3 Parents and volunteers will be made aware that no photos of children should be taken on their own personal mobile device on school outings or trips.

13 ASSESSING RISKS

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

13.2 In common with other media such as magazines, books and video, some material available through the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of internet access.

13.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

13.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

13.5 The Computing Subject Leader will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

13.6 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

14 INTRODUCING THE POLICY TO PUPILS

14.1 Rules for internet access will be posted in all rooms where computers are used.

14.2 Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks before any lesson using the Internet.

14.3 Pupils will be made aware of the SMART e-safety rules at the start of every new Computing unit of work.

14.4 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

15 CONSULTING STAFF

15.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's E-safety Policy and will be provided with a copy of this which is to be kept in their Computing folders.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Senior managers will supervise members of staff who operate the monitoring procedures.

16 MAINTAINING ICT SECURITY

16.1 Personal data sent over the network will be encrypted or otherwise secured. Each teaching member of staff should use an encrypted memory stick to ensure that confidential data is not accessed out of school.

16.2 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

17 DEALING WITH COMPLAINTS

17.1 Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures.

17.2 The school's designated person for Child Protection will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately.

17.3 Pupils and parents/carers will be informed of the complaints procedure.

17.4 Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

17.5 As with Child Protection issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

17.6 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Referral to the police.

18 PARENTS/CARERS SUPPORT

18.1 Parents/carers will be informed of the school's E-safety Policy which may be accessed on the school website and in the school prospectus.

18.2 Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.

18.3 Advice on filtering systems and appropriate educational and leisure activities including responsible use of the internet will be made available to parents/carers.

18.4 Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

18.5 A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safer internet use at home. Parent forums will be run by the school regularly (when necessary) to advise parents on current E-safety issues.

Written by: Jo Gough