# E-Safety Policy

## Bishop Road Primary School

Adopted by: Finance, Buildings, Health & Safety Committee

Adopted: November 2020

Review: November 2022

This policy has been written with consideration of with the following school policies:

- Anti-Bullying Policy, Behaviour Policy, Data Protection Policy, Staff Code of Conduct, Safeguarding, Health and Safety and the school Equalities Plan

# E-Safety Policy 2020

CONTENTS

## 1. Core Principles of Internet Safety

Effective use of the internet is an essential life-skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. As a consequence, a policy is required to help to ensure responsible use and the safety of pupils. This policy applies to both on and off site activity.
This Internet Safety Policy is built on the following core principles:

### 1.1 Guided Educational Use

Significant educational benefits should result from curriculum internet use including access to information from around the world and the ability to communicate widely and to publish easily. Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

### 1.2 Risk Assessment

21st Century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they need to learn to recognise and avoid these risks – to become "Internet Wise". Schools need to ensure they are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Pupils need to know how to cope and respond if they come across inappropriate material.

### 1.3 Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully.

### 1.4 Regulation

The use of a limited and expensive resource, which brings with it the possibility of misuse, must be regulated. Fair rules, clarified by discussion and prominently displayed will help pupils make responsible decisions.

### 1.5 Appropriate Strategies

This document describes strategies to help ensure responsible and safe internet use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities.

## 2. Why is Internet use important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems.

## 3. How will Internet use enhance learning?

• The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
• Pupils will learn appropriate Internet use and be given clear objectives for Internet use.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

## 4. How will Internet access be authorised?

• All staff and pupils will be granted internet access.
• Parents will be informed (via the e-safety section and digital awareness page on the school website) that pupils will be provided with supervised Internet access (example statement is included as an appendix).

- The school wifi password will only be provided to staff members by the IT technician and used in line with this policy.

## 5. How will filtering be managed?

•Primary pupils may not be issued individual email accounts unless monitored accounts, but will be authorised to use a group/class email address under supervision if necessary.
• At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online material.
• The school will work in partnership with parents, Bristol City Council, DfE and the SWGFL to ensure systems to protect pupils are reviewed and improved.
• If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the Computing co-ordinator or Online Safety lead. Parents of the children involved will be notified immediately.
• BCC IT support will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## 6. How will the risks be assessed?

• 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 the LA 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 and Computing leader will ensure that the Internet policy is implemented and compliance with the policy monitored.

## 7. Managing Content

### 8.1 How will pupils learn to evaluate Internet content?

• If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing Coordinator.

• Schools should ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.
• Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources and how they can react appropriately.
• Nominated persons (Computing Coordinator and IT Technician) will be responsible for permitting and denying additional websites as requested by colleagues.

### 8.2 How should website content be managed?

• The point of contact on the website should be the school address, email and telephone number. Staff or pupils' home information will not be published.
• School will obtain all relevant permissions prior to using images of children on the school website.
•Where audio and video are included (podcasts/video blogging) the nature of the items uploaded will no include content that allows pupils to be identified. Content shared by teachers to website co-ordinator will happen through the encrypted school email system.
•The website coordinator and IT technician will take overall editorial responsibility and ensure that the content is accurate and appropriate.

## 9. Communication

### 9.1 Managing e-mail

• 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.
• Whole-class or group e-mail addresses should be used, unless it is a monitored account at Key Stage 2.
• E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

### 9.2 On-line communications and social networking

• At Bishop Road we recognise the essential role of safe online communication. Safe use of the internet and specifically Social Network sites will be taught as part of the computing curriculum.
• Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
• Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
• Pupils will be advised to use nicknames and avatars when using social networking sites as part of the e safety programme.

### 9.3 Mobile phones and other electronic devices

• Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.
• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

• Pupils in Yr 5 & 6 are permitted mobile phones in school providing they are turned off and not used in the school day. There is no arrangement or provision for the storage of mobile devices and school does not accept any liability for loss, damage or theft of any device.

- External flash drives will not be used to store or transport information from home to school. Teachers will only use the school's encrypted Onedrive.

## 10. Use of devices

### Staff use of personal devices

• Staff are not permitted to use their own mobile phones and personal devices for contacting children. Staff should not use personal devices to take photos or videos of pupils and will only use school designated devices for this purpose.
• Staff and volunteers should not use personal mobile phones and other electronic devices for personal reasons whilst they are responsible for children in teaching situations and in the playground. Staff may access their personal devices whilst off duty but not in designated areas used by children.
• During off-site visits, adults should ensure that they have access to a mobile phone and that this is switched on. These should only be used if there is an emergency of if they need to contact the school or other group leaders.
• Where staff members are required to use a mobile phone for school duties, for instance in the case of offsite activities.
*COVID related clause*– Only through exceptional circumstances (e.g. national lockdown or remote learning) will personal devices be used to contact parents and pupils.

### Pupil use of school devices

- Laptops and iPads will be used under the supervision of staff members for specific activities.
- Children will be directly to specific apps or given direct instructions for internet use.

*COVID related clause*- iPads will be cleaned after each use by the class teacher.

### Staff/Adult use of school designated devices

• Only authorised school technology may be used to record children's activities.
• On trips, staff and volunteers should only use school devices for the purpose of taking photographs/videos.
• In school, visitors accompanied by staff may be granted permission to use authorised devices when agreed by a Senior Leader.
• All staff are responsible for the security of electronic devices which have been allocated to them. Devices which store data, children's information or photos must be password protected where possible. Devices must be locked away at the end of the day.

- Ipads are locked in secure units. The keys are kept by the computing co-ordinator and IT technician and signed out to teachers. The key will be returned after use.

### Parent/carers use of personal electronic devices

• Parents/carers visiting the school or volunteering for school trips may not use personal devices to take photos or videos of pupils except when authorised such as class performances and recitals.

• Parents/carers will be given the opportunity annually to inform school of their wishes with regards to the use of images and recordings. School staff are responsible for ensuring they check the school register for any restrictions as per above.

### Pupils' use of personal devices

• Personal mobile phones are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile devices.
Pupils will be provided with appropriate school devices to use in specific learning activities under the supervision of staff.
• Images on pupils' own devices are for personal use only and are not to be uploaded on any social networking sites.
• If a pupil breaches the school policy, then the device will be confiscated and held in a secure place in the school office until the child's parent/carer has met with a member of SLT.
• Teachers are responsible for briefing children on the appropriate use of cameras/phones before any school trip/off site visit.

### Breach of policy

• If an adult breaches school policy, concerns will be taken seriously, logged and investigated appropriately. The Headteacher reserves the right to check the image content of staff's, parent's, visitor's or volunteer's mobile phone or other electronic recording device, should there be any cause for concern over appropriate use. If inappropriate material be found, Child Protection procedures will be initiated.

## 11 . Introducing the Policy to Pupils

• Pupils will be reminded of Rules for Internet access before each session.
• A module on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
• Instruction on responsible and safe use should precede Internet access.
• Pupils will be informed that Internet use will be monitored.
Teaching of e-safety will be reviewed and updated annually or when necessary.

## 12. Parents and E-Safety

• Parents' attention will be drawn to the School E-Safety Policy and Digital Awareness blog in newsletters and on the school Website.
• Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
• Internet issues will be handled sensitively to inform parents without undue alarm.
• A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
• All parents will receive support information as and when available.

## 13. Consulting with Staff and their inclusion in the E-safety Policy

• All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
• The school's consequences for Internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
• All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
• Community users of the school's ICT facilities must agree to the acceptable user policy before being granted access. This is made available to staff on the school server.
• Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

## 14. How will complaints be handled?

• Responsibility for handling incidents will be delegated to a senior member of staff.
• Any complaint about staff misuse must be referred to the headteacher.
• Pupils and parents will be informed of the complaints procedure.
• Parents and pupils will need to work in partnership with staff to resolve issues.
• There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Bishop Road Primary School

# Rules for Responsible Internet Use

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

- I will ask permission before using the internet.
- I will use only my class login and password, which I will keep secret.
- I will only open or delete my own files.
- I will not bring flash drives, CDs or DVDs into school unless I have permission.
- I will only e-mail and open attachments from 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.
- If I see anything I am unhappy with or I receive messages I do not like; I will tell a teacher immediately.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers

Bishop Road Primary School

# Responsible Internet Use Statement

As part of your child's curriculum and the development of their ICT skills, Bishop Road Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. All children begin the academic year learning about e-safety and follow the SMART rules to keep them safe when using the internet. These are displayed around school to remind the children how to use the internet safely and responsibly.

We expect all members of our school community including parents and carers to support our approach to responsible internet use.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of internet use please telephone the school to arrange an appointment with either your child's class teacher in the first instance.

Bishop Road Primary School

Bishop Road, Bristol BS7 8LS

**Head Teacher: Gillian Powe**
Deputy Head Teacher: Joe Emissah

## Pupil Acceptable Use Agreement/e-Safety Rules

Dear Parent/Carer
ICT including the internet, email, laptops, digital cameras etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.
Please discuss these eSafety rules with your child. If you have any concerns, please contact the school which holds an e-Safety policy.

- I will only use ICT in school for school purposes.
- I will only use my class email address (this will only be available for specific lessons as required),
- I will make sure that all ICT contacts with other children and adults are responsible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my monitor and tell my teacher immediately. • I will not send to children or adults anything that could be considered unpleasant or nasty.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.

e-Safety Agreement

Name of child

……Class……

We have discussed this and my child agrees to follow the e-Safety rules and to support the safe use of ICT at Bishop Road Primary School.

Parent/ Carer Signature

……Date……

# Laptop policy for Bishop Road Primary School Staff 2020

1. The laptop remains the property of Bishop Road School.

2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Bishop Road School Staff should use the laptop.

3. On the teacher leaving the school's employment, the laptop is returned to Bishop Road School.

4. Staff on extended leave of 4 weeks and over should return their laptops to the school

(other than by prior agreement with the headteacher).

5. When in school and not being used, the laptop must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.

6. Whenever possible, the laptop must be taken out of school and if so not be left in an unattended car. If there is a need to do so it should be locked in the boot.

7. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.

8. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.

9. Any software loaded must not affect the integrity of the school network.

10. If any removable media is used then it must be checked to ensure it is free from any viruses.

11. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.

12. If any fault occurs with the laptop, it should be referred to the Systems and Services Manager.

13. The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

## Policy for responsible e-mail, network and Internet use for Bishop Road Primary School

1. I will use all ICT equipment issued to me in an appropriate way. I will not:

- Access offensive website or download offensive material.

- Make excessive personal use of the Internet or e-mail.

- Copy information from the Internet that is copyright or without the owner's permission.

- Place inappropriate material onto the Internet.

- Will not send e-mails that are offensive or otherwise inappropriate.

- Disregarded my responsibilities for security and confidentiality.

- Download files that will adversely affect the security of the laptop and school network.

- Access the files of others or attempt to alter the computer settings.

- Update web pages etc. or use pictures or text that can identify the school, without the permission of the headteacher.

- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Bishop Road Primary School.

2. I will only access the system with my own name and registered password, which I will keep secret.

3. I will inform the ICT School's Technician as soon as possible if I know my password is no longer secret.

4. I will always log off the system when I have finished working. ·

5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.

6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the headteacher and register the passwords with the headteacher.

7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.

8. I will not open e-mail attachments unless they come from a recognised and reputable source.

9. I will bring any other attachments to the attention of the ICT technician.

10. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.

11. I will report immediately to the headteacher any unpleasant material or messages sent to me.

12. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.

13. Use for personal financial gain, gambling, political purposes or advertising is forbidden.

14. Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.

15. Activity that threatens the integrity of the school IT systems, or activity that attacks or corrupts other systems, is forbidden.

## Web-based Resources

For Schools

KidSmarthttp: www.kidsmart.org.uk

SMART rules from Childnet International and Know It All for Parents

Childnet International http://www.childnet-int.org

Guidance for parents, schools and pupils

Bectahttp: www.schools.becta.org.uk/index.php?section=is

e-Safety Advice

Becta / Grid Club, Internet Proficiency Scheme. On-line activities for Key Stage 2 pupils to teach e-safety. http://www.gridclub.com/teachers/t_internet_safety.html

South West Grid for Learninghttp: www.swgfl.org.uk/onlinesafety

DfE Anti-Bullying Advice http: www.gov.uk/governmnet/publications/preventing-and-tackling-bullying

Grid Club http://www.gridclub.com/teachers/t_internet_safety.html

Internet Watch Foundation www.iwf.org.uk

Invites users to report illegal Websites

South West Grid for Learning - Safe www.swgfl.org.uk/safe

A comprehensive overview of web-based resources to support schools, parents and pupils

Think U Know www.thinkuknow.co.uk/

Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

## For Parents

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspx

A downloadable PowerPoint presentation for parents

Childnet International http://www.childnet-int.org/

## 17. Notes on the Legal Framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice)

(Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of, amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others.

Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following the signing of an agreement to use the equipment under the conditions as laid out by the school. (A copy of the Council's policy is included in section 15). The Rules for Responsible Internet Use, to which every user must agree, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring. For example, each school can review the websites visited by the school each day / week / month. Though this is not user specific it does allow a degree of monitoring to be conducted. All schools are also able to monitor school e-mail.

Cyber-stalking & Harassment (http://wiredsafety.org/gb/stalking/index.html)

Under Section 1 of the Malicious Communications Act 1998 it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person and under Section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent, offensive or threatening. In both cases the offence is punishable with up to six months' imprisonment and/or a fine of up to £5000. As the Malicious Communications Offence is more wide-ranging than the Telecommunications offence it is more likely to be used by the Police than the Telecommunications Act offence.

In most cases involving malicious communications or cyber-stalking however there will be more than one offensive or threatening letter or telephone call and therefore the police will often choose to charge the offender with an offence contrary to Section 2 of the Protection from

Harassment Act 1997; also punishable with up to six months' imprisonment. Part of the reason for using this charge is that when someone is convicted of an offence under the Protection from

Harassment Act 1997 the court can make a Restraining Order preventing them from contacting their victim again. Breach of a Restraining Order is punishable with up to five years' imprisonment. A Restraining Order cannot be imposed for a conviction under the Malicious Communications or Telecommunications Acts.

If the e-mails, cyber-stalking etc. causes the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary to Section 4 of the Protection from Harassment Act 1997 which is punishable with up to five years' imprisonment and also allows the court to make a Restraining Order.

If the e-mails, cyber-stalking etc. is racist in nature or motivated by religious hostility then charges could be brought of Racially or Religiously-Aggravated Harassment contrary to Sections 32(1)(a) or

32(1)(b) of the Crime and Disorder Act 1998. If convicted offenders could face up to7 years' imprisonment.

The fact that an offensive telephone call, letter e-mail etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In addition they may justify a claim for constructive dismissal and compensation under employment law.

In many situations the recipient of malicious messages knows who the sender is. It may be a former partner or a relative which may mean that the victim is reluctant to involve the police. In those circumstances the victim could consider taking out an Injunction under Section 3 of the Protection from Harassment Act 1997. However we would always advise

informing the police especially if the messages are in any way threatening. Even if the police decide not to prosecute they may give the offender a formal warning which could be used in evidence if they repeated their behaviour in future.

In addition to criminal prosecutions victims of harassment can sue the offender under Section 3 of the Protection from Harassment Act 1997 for damages arising out of the anxiety caused by the harassment and any financial loss it caused.