**Abbey Primary School, Shaftesbury - E-Safety Policy**

**Introduction**

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

The internet allows access to a vast range of useful resources and information, and is undoubtedly revolutionising education. However there is material available which can be harmful both to children and adults. It is our duty to do our best to ensure that staff and children have access to the valuable internet resources while protecting them from potentially dangerous aspects.

**Internet use guidelines**

* + Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity. Pupils should not be allowed to freely surf without guidance and direction.
	+ Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. If pupils encounter material they find distasteful, uncomfortable or threatening, they must close the page and report the URL to the teacher or ICT manager for inclusion in the list of blocked sites.
	+ It is essential that children are never allowed unsupervised internet access.

**Internet policing**

* + Internet access in school is filtered by RM safetynet (SWGfL). This ensures that the majority of inappropriate material is not accessible in school. However it is also important that staff closely monitor children’s use. Inappropriate use of the internet, for example searching with inappropriate words, should result in a temporary or permanent ban of internet use by the pupil(s) involved. If staff or pupils accidentally discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
	+ Neither the school nor Dorset 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.
	+ Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
	+ Instruction in responsible and safe use should precede internet access. Staff sign an acceptable use agreement each year and children sign a class acceptable use agreement in conjunction with class discussion about safer internet use.
	+ Pupils should be informed that their internet use will be monitored.
	+ Sites visited by staff and pupils are monitored and recorded by SWGfL. Access to some of these records has recently been made available to ICT coordinators.
	+ Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
	+ The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures will be supervised by senior management.

**Judging internet content**

* + Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
	+ Pupils should be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

**Email**

* + 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, such as address or telephone number, or arrange to meet anyone using e-mail communication.
	+ E-mail sent to an external organisation should be written carefully and authorised before sending.

**School Website**

* + Web site photographs that include pupils should be selected carefully and must not include children on the schools non-permitted photograph list. Large detailed portrait pictures will not be used.
	+ Pupils’ full names must not be used alongside photographs.

**Pupil websites**

* + Children must not put personal details on their websites.
	+ Any form of teasing, bullying or harassment is strictly forbidden.
	+ When publishing material to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material.

**Chat rooms and social networking:**

* + Social networking sites for example ‘Instagram’, ‘Snapchat’, or ‘Facebook’, are not to be used in school.
	+ Children should use only regulated educational chat environments in school. This use must be supervised and the importance of chat room safety emphasised.

**Photographic, video and audio technology**

* + Children use cameras but must be taught to treat them with great care; camera straps should be around wrists or necks whenever possible. Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed. It is not appropriate to use photographic or video devices in changing rooms or toilets.
	+ Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities.
	+ Audio or video files may only be downloaded in school if they relate directly to the current educational task being undertaken.
	+ Pupils must always seek the permission of their teacher before making audio or video recordings within school.
	+ Staff know that they must follow the Abbey Primary Code of Conduct for use of cameras.

Mobile phones/new technologies.

* + The move towards combined pocket sized computer/communication/entertainment devices means a constant review of what is relevant in the school environment. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
	+ Pupil mobile phones are only allowed in school following specific discussions between parents and staff, where a specific need has been identified.
	+ Staff know that they must follow the Abbey Primary Code of Conduct for use of mobile phones

**Policy distribution**

* + All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School e-Safety Policy, and have its importance explained.

 A signed sheet will ensure that all Staff have read it.

* + Parents’ attention will be drawn to the policy in newsletters, the school brochure and on the school website.

**System security**

* + Good practice requires logging out when away from a computer.
	+ Virus protection will be installed and updated regularly. Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school by children without specific permission and a virus check.
	+ Unapproved system utilities and executable files will not be allowed in pupils’ work areas or attached to e-mail. Pupil files held on the school’s network may be checked by staff at any time.
	+ Pupils may only log on with their class account, unless given specific permission otherwise by staff. Pupils must not attempt to access the files of other children or adults without their permission.

**This policy was reviewed and readopted October 2022**

This policy should be read in conjunction with the Single Equality Policy. The general equality duty requires that, in the exercise of their functions, schools must have due regard to the need to eliminate unlawful discrimination, harassment, victimisation and other conduct prohibited by the Equality Act 2010. This school endeavours to advance equality of opportunity and foster good relations for all.

External Web Sites:

DFES SUPERHIGHWAY INTERNET SAFETY SITE

http://www.safety.ngfl.gov.uk/

PARENTS ON-LINE DfES WEB SITE

http://www.parentsonline.gov.uk/2003/parents/safety/index.html

BECTA – WHAT IS GOOD PRACTICE IN INTERNET SAFETY

Information sheet

http://www.ictadvice.org.uk/index.php?section=ap&rid=455&catcode=as\_pl\_acc\_03

BECTA – WHAT IS AN ACCEPTABLE USE POLICY

Information Sheet for Teachers and Schools

http://www.ictadvice.org.uk/index.php?section=ap&rid=463&catcode=as\_pl\_acc\_03

BECTA – WHAT ARE MANAGEMENT ISSUES OF TEACHER ACCESS TO THE WEB & EMAIL

Information sheet for Teachers and Schools

http://www.ictadvice.org.uk/index.php?section=ap&catcode=as\_pl\_acc\_03&rid=461&wn=1&pagenum=1&NextStart=1

BECTA – WHAT IS THE ROLE OF THE SCHOOL IN ENSURING SAFE ACCESS TO THE INTERNET

Information sheet for Teachers and Schools

http://www.ictadvice.org.uk/index.php?section=ap&catcode=as\_pl\_acc\_03&rid=462&wn=1

BECTA – WHAT IS GOOD PRACTICE IN INTERNET SAFETY

Information sheet for Teachers and Schools

http://www.ictadvice.org.uk/index.php?section=ap&catcode=as\_pl\_acc\_03&rid=455&wn=1

The Law:

􀂄THE COMPUTER MISUSE ACT 1990

http://www.ja.net/CERT/JANET-CERT/law/cma.html

􀂄THE DATA PROTECTION ACT

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

􀂄THE COPYRIGHT, DESIGNS AND PATENTS ACT 1988

http://www.hmso.gov.uk/acts/acts1988/Ukpga\_19880048\_en\_1.htm

Equality Impact Assessment – initial screening record

|  |  |
| --- | --- |
| 1. What area of work is being considered? | E Safety Policy |
| 2. Upon whom will this impact? | Whole School Community |

3. How would the work impact upon groups; are they included and considered?

|  |  |  |  |
| --- | --- | --- | --- |
| ***The Equality Strands*** | Negative impact | Positive impact | No impact |
| Minority ethnic groups |  | X |  |
| Gender |  | X |  |
| Disability |  | X |  |
| Religion, Faith or belief |  | X |  |
| Sexual Orientation  |  | X |  |
| Transgender |  | X |  |
| Age (N/A to pre-school and school children) |  | adults |  |
| Rurality |  | X |  |

4. Does data inform this work, research and/or consultation, and has it been broken down by the equality strands?

|  |  |  |  |
| --- | --- | --- | --- |
|  | NO | YES | Uncertain |
| Minority ethnic groups |  | X |  |
| Gender |  | X |  |
| Disability |  | X |  |
| Religion, Faith or belief |  | X |  |
| Sexual Orientation  |  | X |  |
| Transgender |  | X |  |
| Age |  | X |  |
| Rurality |  | X |  |
| Does the initial screening highlight potential issues that may be illegal? YES / NO |
| Further comments:- Work with the Safer Communities Police programme and Safer Internet Days back up this policy. |
| Do you consider that a full Equality Impact Assessment is required? YES / NO |
| Initial screening carried out by Mr Michael Salisbury Signed Michael Salisbury Date: 7th October 2022  |

|  |
| --- |
| Comment by Headteacher:Date…………………. |