Policy for E safety

at

WESTON ALL SAINTS PRIMARY SCHOOL

Bath and Mendip Partnership Trust

Review Due: March 2022
Last review: March 2018

Any named persons in this policy are outlined below:

Name	Role
Sharon Badger	Deputy Headteacher

1. E-Safety Policy

1.1 E-Safety encompasses electronic and Internet technologies and communications such as mobile phones, tablets, games consoles and other technology. It highlights the need to educate children and young people about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

1.2 As with all risks it is impossible to completely eliminate them. It is therefore essential that we assist students, staff and parents in acquiring the skills with which they can remain safe while using technology.

1.3 Weston All saints Primary School has appointed an E-Safety Coordinator and Designated Safeguarding Leads. Our E-Safety Policy has been written by the trust in agreement from the senior management team and approved by The Board of Directors.

2. Aims

2.1 The aim of the E-Safety policy is to promote the effective and safe use of technology throughout the Trust, preparing children to the modern world so that they are good digital citizens and can manage their access to and use of technology including the internet.

2.2 Internet use is part of the curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use.

2.3 Our School has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.4 Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;

- professional development for staff through access to national developments,
- educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority;
- access to learning wherever and whenever convenient.

3. Strategies

3.1 E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the SWGFL including the effective management of content filtering.

3.2 The purpose of Internet use in school is

- to raise educational standards,
- to promote pupil achievement,
- to support the professional work of staff
- to enhance the school's management of information and administration systems.

3.3 The school Internet access will be designed expressly for pupil use and therefore includes filtering appropriate to the pupils.

3.4 As part of our computing lessons pupils are taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

3.5 The school will work in partnership with the Local Authority and SWGFL to ensure filtering systems are as effective as possible. SWGFL blocks/filters access to social networking sites and newsgroups unless a specific use is approved

3.6 The Trust will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

3.7 Neither the school nor LA can accept liability for the material accessed, or any consequences or Internet access.

3.8 The school will audit IT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.

3.9 School IT systems capacity and security will be reviewed as and when is needed.

3.10 Virus protection will be installed and updated regularly and security strategies will be in line with the Local Authority.

3.11 Emerging technologies will be examined for educational benefit before use in school is allowed.
3.12 Use of personal mobile phones and other handheld devices for taking pictures and video footage by staff is discouraged but permitted providing staff upload and then delete the images from their phones and handheld devices, as we make required technologies available when possible.
3.13 Pupils who are on our media alert will not have photographs published on the school website or have worked displayed with their surname on it.
3.14 Photographs that include pupils will be selected carefully in line with our 'Media-Alert system and will not display pupil surnames.
3.15 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4 Safe/ Acceptable Use

4.1 Pupils

4.1.1 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities.
4.1.2 Pupils are not permitted to have mobile phones in school unless consent is granted by the head teacher. In this instance the mobile phone must be handed in to the school office and collected at the end of the school day.
4.1.3 Staff and pupils personal information will not be published by the school.
4.1.4 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils may only use approved e-mail accounts on the school system.
4.1.5 Pupils must immediately tell a teacher if they receive offensive e-mails.
4.1.6 Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
4.1.7 All parents and pupils must read and sign the ‘E-safety Pupil Contract’
4.1.8 If pupils discover unsuitable sites, they must click on ‘Hector the dolphin’ and report to a member of staff.

5 Cyberbullying/ Safeguarding

5.1 The school takes cyberbullying and incidents similar to this very seriously.
5.2 The school, as much as is reasonable, has a responsibility to educate and regulate children in their online behaviour and any behaviours/ incidents that are brought into school.
5.3 The school will follow our Positive Behaviour Management and Anti- bullying policies when dealing with any incidents and consequences as appropriate.
5.4 Cyberbullying can occur through many forms and includes (but is not exclusively):

- Sending communication, posts, comments (including words, images, audio and video) that may be upsetting, threatening and/or abusive, through mobile phones, social media, chatrooms, emails and other technologies
- Sharing media content of an individual or group without their consent for negative or derogatory reasons
- Any persons using any technology to post unwanted communication (see bullet point 1) about the school, staff or pupils, thus bringing the school into disrepute, is a disciplinary offence and will be dealt with accordingly.

6 Staff

6.1 Staff and pupils receive guidance relating to the use of Facebook and other social networking sites, personal safety and security; age appropriate material will be shared with them.
6.2 Staff and pupils' personal information will not be published by the school
6.3 Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
6.4 All staff have read and sign the 'Acceptable IT Use Agreement' before using any school IT resource.
6.5 Staff should guide pupils before using any school IT resource.
6.6 If staff discover unsuitable sites, the URL (address), time, content must be reported to the SWGFL helpdesk via the E-Safety Coordinator.

7 Visitors

7.1 Visitors are permitted to bring their own device (BYOD) on to school premises. They may be given access to the school guest network at the discretion of the appropriate staff member.
7.2 When doing so, visitors must be sure that their device is virus free and be aware that their use of the school network will be monitored in line with the school policy.
7.3 The school reserves the right to ask visitors to stop using their device and to remove any data collected or generated while on site.

8 Complaints/Misuse

8.1 Complaints of Internet misuse will be dealt with by a senior member of staff.
8.2 Any complaint about staff misuse must be referred to the Executive Headteacher.
8.3 Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.
8.4 Pupils and parents will be informed of the complaints procedure.
8.5 If materials that are deemed unsuitable by this policy are accessed, the school will report this issue direct to the filtering provider and will be dealt with as a safeguarding matter.

9 Guidance

Further E-Safety guidance can be found on our website www.wasp-school.org.uk with several links to the latest E-safety guidance for pupils and parents.

10 Communication of Policy

10.1 Pupils

- Rules for Internet access will be shared with pupils.
- Pupils will be informed that Internet use will be monitored.

10.2 Staff

- All staff will be given the relevant E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

10.3 Parents

- Parents’ attention will be drawn to the relevant E-Safety Policy on the school websites.

10.4 Any persons using any technology to post unwanted communication (see bullet point 1 in cyberbullying section) about the school, staff or pupils, thus bringing the school into disrepute, is a disciplinary offence and will be dealt with accordingly.