E-Safety policy

Meare Village Primary School

Approved by:	Jan Fellows Headteacher	**Date:** April 2019
Last reviewed on:	April 2019	
Next review due by:	April 2023	

1. Reviewing the e-Safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including anti-bullying and safeguarding children protection.

- The school has an appointed an e-Safety Coordinator who will attend appropriate training and will provide support and training for all staff and volunteers.
- Our e-Safety Policy has been written by the school, building on guidance from Somerset LA and the Government. It has been agreed by senior management and approved by governors.
- The e-Safety Policy is reviewed annually by: the Senior Management Team, e-Safety/IT Co-ordinator and Welfare Committee Governors.

2. Teaching and learning

2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. (see 3.6 below)
- Pupils will be taught what Internet use is acceptable and what is not and 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.

2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations acknowledging sources of information used
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Internet Access

3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- The security of the school network relies on the central firewall implemented by SWGfL. No traffic shall enter or leave the SWGfL Infrastructure without being explicitly permitted by the firewall. No traffic shall route directly between connected establishments unless it has been explicitly allowed to do so. The configuration of the firewall can be changed at the request of the school when a security review will be conducted and advice taken from SWGfL. (see also SWGfL Security Policy)
- Websites are only accessed through Proxy Servers provided by Somerset.
- Password security is of the utmost importance and must be maintained at all times. Adults and children will be reminded never to disclose their passwords. The abuse of passwords must be reported immediately to the e-Safety coordinator and recorded in the e-Safety log.

3.2 Managing filtering

- Developing good practice in internet use as a tool for teaching and learning is essential. School internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children. They will be taught about this filtering process.
- The school will work with the LA, SWGfL, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. An enhanced version of RM SafetyNet Plus is deployed by SWGfL to filter the Internet stream to the school.
- Pupils (and staff) will be taught what to do if they experience material they find distasteful, uncomfortable or threatening. This will be recorded in the e-Safety log and reported to the e-Safety Coordinator and the URL and content will be reported to the SouthWest One helpline.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.3 On-line working and communication

- All pupils have access to a personal online learning space which will be used for communication, collaboration and publishing to support pupils' learning
- The school will control access to moderated social networking sites and educate pupils in their safe use.
- The South West Grid for Learning will block/filter access to other social networking sites such as Facebook and to chat rooms.
- Pupils will be taught the importance of personal safety when using social networking sites and chat rooms. They will be advised never to give out personal details of any kind which may identify them or their location. They will be advised to use appropriate nick names and avatars when using social networking sites.
- Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Materials which victimise or bully someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented. Any misuse will be recorded in the e-Safety log.
- Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.
- Pupils and parents will be advised about inappropriate use of social network spaces outside school.

3.4 E-mail

- Pupils may only use approved e-mail accounts (which do not personally identify them) on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail and this will be recorded in the e-Safety log.
- Pupils must not reveal personal details of themselves or others in e-mail communication. Arrangements to meet anyone will only be where it is part of a school project and pupils are working under the supervision of their teacher.
- Personal e-mail or messaging between staff and pupils should not take place.
- Staff must use and LA/School approved VLE or email solution when they need to communicate with pupils about their school work.
- Pupils will be taught appropriate, sensible and responsible use of e-mail.
- 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.
- The forwarding of chain letters is not permitted.

3.5 Published content and the school web site

- 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.
- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.6 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

3.7 Managing videoconferencing (not applicable currently)

- Video conferencing is only enabled through the SWGfL Gatekeeper.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. .
- Staff will be issued with a school phone where contact with pupils is required.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4 Policy Decisions

4.1 Authorising Internet access

- All staff will sign the 'Acceptable ICT Use Agreement' on the South West Grid for Learning website http://www.swgfl.org.uk/staying-safe before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At key stage one children's experience of the Internet will be through adult demonstration and access to websites under the supervision of an adult.

4.2 Assessing risks

- 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 Our education programme for Internet Safety with pupils will give them clear strategies and processes for dealing with anything they find online that causes them to feel uncomfortable.
- The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

5 Communicating the Policy

5.1 Introducing the e-Safety policy to pupils

- E-Safety rules will be discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored and that misuse will be dealt with appropriately.
- Pupils will sign an acceptable use policy (see 5.3).
- Pupils will be taught appropriate and responsible behaviours for using the Internet and communication tools within PSHE and across the curriculum. Misuse will be recorded in the e-Safety log.
- 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.

5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained. This will be part of the induction process for any new member of staff.
- Staff are made aware that Internet traffic is monitored by SWGfL and traced to the individual user. Any potential misuse as set out in the SWGfL Internet Acceptable use policy will be reported to the school**.** Discretion and professional conduct is essential.

5.3 Enlisting parents' support

- Parents will be asked to read through an acceptable use policy with their child. This will be signed by pupil and parent and returned to school.
- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

6 Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-Safety.

- The school's ICT resources may be used by community groups. All adult users will sign the SWGfL acceptable use policy and will be aware of the school's e-Safety policy.
- Parents/carers of children and young people who are not members of the school will be required to sign the acceptable use policy on behalf of their child or young person under the age of 16.

7 Handling e-Safety complaints

- The staff, children and parents/carers will know how and where to report incidents (e-Safety coordinator, e-Safety log and CEOP Child Exploitation and Online Protection Centre).
- Concerns related to Safeguarding issues will be dealt with through the school's Safeguarding Policy and Procedures.
- Complaints of Internet misuse will be dealt with by a senior member of staff in accordance with the schools behaviour policy.
- Any complaint about staff misuse must be referred to the headteacher.
- Sanctions for pupil misuse may include:
    - Informing parents/carers
    - Removal of internet/VLE access and or ICT equipment for a specified period of time.