Much Marcle C E Primary School

E-safety Policy

Date Reviewed	Reviewed By	Next Review
October 2017	Lorna Harrison	October 2019

TEACHING AND LEARNING

Why the Internet and digital communications are 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.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

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.

- 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.

- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

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

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet content eg using the CEOP Report Abuse icon or Hector Protector.

MANAGING INTERNET ACCESS

Information system security

- Security strategies will be discussed with Edutech, our IT provider.

- School ICT systems security will be reviewed regularly by Edutech.

- Virus protection will be updated regularly by Edutech.

Email

- Pupils may only use approved e-mail accounts on the school system with the full knowledge of their teacher.
- The school do not let pupils email external bodies without the presence of a teacher.
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- Pupils must immediately tell a teacher if they receive offensive email.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

Publishing pupil's images and work

- Photographs that include pupils will be carefully selected so that individual pupils cannot be identified or their image misused.
- Pupils' full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location and are advised not to meet with anyone they have met on the internet.

- 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 age-appropriate social networking sites and online gaming.

- Pupils and parents are advised about the age restrictions on social networking site and the dangers of their use for younger children.

Managing filtering

- The school will work with the Edutech, CEOP and Becta to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the headteacher, Edutech and CEOP.

- Edutech will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Staff should check any sites that they intend to direct pupils to during lessons to ensure the content is appropriate.

Managing videoconferencing and webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.

- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

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.

- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

- The use by pupils of cameras on mobile phones will not be allowed.

- Games machines including the Sony Playstation, Microsoft Xbox and others that have Internet access which may not include filtering will not be used in school.

- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

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

POLICY DECISIONS

Authorising Internet access

- All staff must read the 'Staff Code of Conduct' before using any ICT in school.

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

- Any person not directly employed by the school will be asked to read this policy and the Staff Code of Conduct before being allowed to access the internet from the school site and will use the visitor log in – Visitor – Mvisit01.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Edutech can accept liability for any material accessed, or any consequences of Internet access.

- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the head teacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures outlined in the Safeguarding Policy and Child Protection Policy.

- Pupils and parents will be informed of the complaints procedure.

- Pupils and parents will be informed of consequences for pupils misusing the Internet.

COMMUNICATIONS POLICY

Introducing the e-safety policy to pupils

e-Safety rules will be posted in all classrooms, Ipad and Laptop trolleys and in the library. These rules will be discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.

e-Safety training will be embedded within the Computing scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web s

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

I will ensure my mobile phone is kept in the staff room when children are on the premises.

I will not use my mobile phone in the classroom or in front of pupils.

I will not use my mobile phone to take photographs of pupils.

I understand that school information systems may not be used for private purposes without specific permission from the head teacher.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

I will not install any software or hardware without permission.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the e-Safety Co-ordinator, the Designated Safeguarding Lead (Head Teacher) or the Deputy Safeguarding Lead.

I will not have any electronic communications with pupils including email, IM and social networking.

I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.