Madley Brook CP School

e-Safety Policy

Introduction
E-Safety encompasses Internet technologies and electronic communications such as mobile phones, tablets, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
The school's e-safety policy should operate in conjunction with other policies including those for pupil Behaviour, Bullying, and Safeguarding.

End to End e-Safety
E-Safety depends on effective practice at a number of levels:

- Responsible computing use by all staff and students; 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 including the effective management of filtering systems.

1.0 School e-safety policy

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for computing curriculum and for Safeguarding.

- The school's e-Safety Coordinator is also the computing Subject Leader. He works in close co-operation with the headteacher. The headteacher is one of the school's Designated Safeguarding Leads.
- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.
- E-Safety issues are included in the Safeguarding policy.

1.2 Teaching and learning

1.2.1 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.

1.2.3 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.

- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school Computing Subject Leader.
- Staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1.3 Managing Internet Access

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

1.3.2 Use of E-mail (where applicable)

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.
- Whilst we recognise that some members of staff who live and work within our local community and have friendships with parents as a result of this, any work-related correspondence should be undertaken through school email addresses and not through personal email or phone numbers. (See also 1.3.5)

1.3.3 Published content and the school web site

- 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.

1.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, 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.

1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Contact between staff members and pupils and parents on social networking sites is deemed inappropriate. (See also 1.3.2)
- Class Dojos and Homeroom are monitored by school staff

1.3.6 Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- The Computing Subject Leader will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing iPads

- The Computing Subject Leader will keep the operating system and apps updated and monitor their use regularly.
- Internet access will be filtered through our Internet settings, which are monitored and controlled by the Computing Subject Leader and our technical support partner.
- Staff should guide pupils in using apps and Internet sites that will support the learning outcomes planned for the pupils' age and maturity.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.

1.3.8 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. The sending of abusive or inappropriate text messages is forbidden.
- Staff have access to a school phone where contact with pupils or parents is required. Staff may not use personal mobile phones to contact parents except on an offsite visit, where this is deemed necessary, and access to a school phone is not possible.

1.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

1.4 Policy Decisions

1.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Teaching Assistants must read and sign the acceptable computing Code of Safe Practice before using any school computing resource.
- At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Code of Safe Practice.

1.4.2 Assessing risks

- 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

1.4.3 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 Safeguarding nature must be dealt with in accordance with school Safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions within the school behaviour policy include:
  – discussion with class teacher / headteacher;
  – informing parents or carers;
  – removal of Internet or computer access for a period.

1.4.4 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms and on mobile computer trolleys.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

1.5.2 Staff and the e-Safety policy

- All staff will be given the School 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.

1.5.3 Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters.
- Parents will be invited to attend E-Safety workshops which will be held in school periodically.

Reviewed May 2019
Also to be read with acceptable use policies for staff and children

E-Safety Audit

This quick audit will help the senior leadership team (SLT) assess whether the basics of e-Safety are in place to support a range of activities that might include those detailed within the ICT curriculum policy.

The school has an e-Safety Policy.	Y
Date of latest update:	
The Policy was reviewed by governors on: **May 15th 2019**	
The Policy is available for staff.	Y
And for parents.	Y
The Designated Safeguarding Leads are: **Katherine Spencer,** Angie Burnett, Iain Curtis, Emma Cuthbertson, Ben McPherson	
The e-Safety Coordinator is **Iain Curtis**	
How is e-Safety training provided? Staff meeting and Inset Time Induction of new staff	
All staff sign an Acceptable Computing Code of Safe Practice.	Y Re-signed May 2019
Parents sign and return an agreement that their child will comply with the school Code of Safe Practice statement.	Y Re-issued Jan 2018
Rules for Responsible Use have been set for pupils.	Y
These Rules are displayed in all rooms with computers	Y
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	Y
The school filtering policy has been approved by SLT.	Y
A computing security audit has been initiated by SLT, possibly using external expertise.	Y
School personal data is collected, stored and used according to the principles of the Data Protection Act	Y
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT.	Y
Have these staff attended training on the filtering and monitoring systems?	Y