OPEN HEARTS · OPEN MINDS · OPEN DOORS

Mobberley C of E Primary School
e-safety Policy

"Open Hearts, Open Minds, Open Doors"
"Ask and it will be given to you; seek and you will find; knock and the door will be opened to you." – **Matthew 7:7**

Mobberley C of E Primary School is a vibrant learning community which promotes excellence and enjoyment, enabling all to fulfil their potential and lead useful, productive and happy lives.
As a Church of England school we aim to provide a place where each child feels safe, respected and valued as an individual.

Policy development

The e-safety policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-bullying and Safeguarding children.

- Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- It has been agreed by senior managers and approved by governors
- The policy and its implementation will be reviewed annually
- It is available to read or download on our school website or as a hard copy from the school office.

Roles and responsibilities

The school has an e-safety coordinator (in some cases this will be the Designated Safeguarding Lead as the roles may overlap). Our coordinator is: Damien Stenson.

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- Mobberley C of E Primary School has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact. This will include using the CEOP icon or the Hector Protector function.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self –efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

Managing Internet Access

Information security system

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority

E-mail

- Staff may only use approved e-mail accounts on the school system.
- Pupils do not have school email accounts.
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published.
- The headteacher or their nominee will have overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified.
- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission will be obtained from parents and carers before any photographs are published on the school website.
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and educating students in their use
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

Managing filtering

- The school will work with the County Council to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the e-safety coordinator.
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.

Managing video conferencing

- Video conferencing will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a video conference call.
- Video conferencing will use the educational broadband network to ensure quality of service and security.

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required.

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 and sign the 'staff code of conduct' before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are given access to school IT systems
- Parents will be asked to sign and return a consent form
- Access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.
- Any person not directly employed by the school will be asked to read and sign our 'Acceptable Use Policy' before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if 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.
- Complaints of misuse by staff will be referred to the headteacher.
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the schools behaviour policy.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the e-safety policy.

Communicating the policy

Pupils

- Appropriate elements of the e-safety policy will be shared with pupils.
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- All staff will be given a copy of the e-safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting.

Parents

- Parents will be notified of the policy in newsletters, the school brochure and website.
- All parents will be asked to sign the parent/pupil agreement when they register their children.
- Parents will be offered e-safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

This E-safety policy was revised by: Kirsty Ruddle
On (date): September 2026

To be reviewed September 2027