# St Matthew's Primary School

# eSafety Policy

Date Policy Written: Originally Written 2017.
Reviewed Oct 2025 Review Cycle: Annual basis or
sooner if required.
Ratified by Governing Board on: 15th July 2024
Next review date: Oct 2026
This Policy should be read in conjunction with: Social Media & Internet Acceptable Use Policy, Information Security Policy.

**Policy Overview**

eSafety encompasses Internet-based technologies used for electronic communications such as mobile phones, smart tablets, laptops and PC's. It highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory 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. 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.

**Policy Links**

The school's eSafety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Child Protection, Safeguarding Children, Curriculum, Data Protection and Security, Confidentiality.

eSafety 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 eSafety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband for learning including the effective management of content filtering.
- National Education Network standards and specifications.

eSafety guidelines apply to all internet-enabled devices, including but not limited to: PCs, laptops, webcams, digital video equipment, digital cameras, multimedia devices, mobile phones, portable media players, games consoles, personal digital assistants and smart tablets (*this list is not exhaustive as new devices are acquired frequently*). All persons either

using technology or supervising the use of technology are required to abide by this policy.

eSafety requirements relate to school-owned technology and also to personal technologies.
eSafety requirements are applicable during the times whereby the school is opened; this applies to term-time, holidays when the school is open, and any extended school events. It is also relevant to residential/off-site events e.g. school trips and visits.

**Designated Person for ESafety Policy**

The school will appoint an eSafety coordinator. In many cases this will be the Designated Child Protection Officer as the roles overlap. The eSafety Coordinator is Sandie Gonsalves.

**Internet: The Benefit to Education**

The Internet will be used to support the schools' implementation and delivery of a Curriculum designed to enhance learning opportunities, including;

- Access to world-wide educational resources.
- Inclusion in the National Education Network which connects all UK schools.
- Educational and cultural exchanges.
- 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.

**Other benefits of the Internet include;**

- Collaboration across support services and professional associations.
- Exchange of curriculum and administration data with the Local Authority.
- Internet access designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- The education of pupils as to what Internet use is acceptable and what is not.
- The education of pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Enriched and extended learning activities and opportunities.

- Staff-guided online activities that will support learning outcomes planned for the pupils' age and maturity

**Authorised Internet Access**

- Our school will comply with copyright law.
- The school will maintain a record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'ICT Acceptable Use Policy" before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.

**Safeguarding Children and Child Protection**

This policy is an extension of the safeguarding children and child protection policies. Caution is expressed to the whole school community with regards to child safety in the virtual world as well as the real world. Social networking sites, the uploading of inappropriate web content and cyber-bullying are issues that adults must ensure vigilance around. Appropriate means are put in place to safeguard and educate our children. It is expected that children are able to develop their own protection strategies for when adult supervision and technological protection are not available.

**World Wide Web**

- If staff or pupils discover unsuitable sites, the URL (address), time & content must be reported to the ICT Network & Data Manager and the event logged on CPOMS for the Safeguarding Lead if the content found requires this.
- The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

**Email**

- Pupils may only use approved e-mail accounts provided by the school; we use Google Suite (Gmail) for this.
- 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.
- Access in school to external personal e-mail accounts may be blocked by the filtering system as a measure of network security.

- E-mail sent to external organisations should be written carefully and, if required, authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain letters is not permitted.

**Social Networking**

- LGfL Filtering blocks access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be advised not to place personal photos on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

**Filtering**

The school will work in partnership with LGfL Filtering to ensure that the Internet filtering systems are as effective as possible. Staff-level filtering is accessible only by a staff LGfL account using an additional username & password unique to each staff member. Pupils cannot access this from any of their computers.

**Video Conferencing**

- Conference call websites will only be available at the discretion of the school and only at staff level of internet filtering.
- Staff should be vigilant about video conference programs and if in any doubt, seek advice from the IT Manager.
- Videoconferencing 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 (usually by the ICT Dept.) before use in school is allowed.
- Personal mobile phones, tablet devices and handheld games consoles must not be used by staff or pupils during lessons or formal school time. Staff use of these devices should be limited to the staffroom and other isolated areas away from pupils.

- Staff use of Mobile Phones should be limited to spaces pupils are not present. Other limited uses for personal mobile phones are not outlines in our 'use of mobile phone risk assessment'.
- Staff will be issued with a school phone where contact with pupils, families, external companies and other organisations is required on school trips.

**Health and Safety concerning technology and devices**

- Pupils' time on devices will be limited and monitored and breaks should be taken when use extends beyond 1 hour of screen time.
- Pupils should not carry or move more than 2 devices at a time; pupils should not move trolleys of equipment.
- Any technological device will give off a variety of signals; WiFi, Bluetooth, Infared etc. To date, no data has shown that proximity to & use of these devices has impacts on health relating to these signals.

**Published Content and the School Web Site**

- The contact details on the school website should be the school address, general e-mail and telephone number. Staff or pupils personal information will not be published, neither will direct contact information unless legally required.
- The Headteacher (*or internal nominee*/s) will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing Pupils' Images and Work**

- Pupils' full names will not be used anywhere on the website or blogs, particularly in association with photographs except in exceptional circumstances where parental permission will be sought. This permission is obtained on entry to the school.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' work will be reviewed for suitability before it is published on the website and/or blog.

**Information System Security**

- The ICT Network & Data Manager will review the schools' computer systems capacity, physical security, data security and network use on a regular basis.

- Anti-virus protection and encryption software will be installed and updated regularly.
- Further information can be found in the "Data Protection Policy".

**Protecting Personal Data**

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

**Assessing Risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and constantly growing nature of the Internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. St Matthew's Primary School cannot accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate.
- Pupils will be taught what to do if they encounter any undesirable Internet content as part of their eSafety lessons.

**Handling eSafety 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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and the schools' Safeguarding policy.

**Communication of the Policy**

- The rules for Internet access and eSafety advice will be on included in computing lessons.
- Pupils will be informed that all Internet and Computer use will be monitored.

**Staff**

- All staff will be given the School eSafety Policy and its importance explained.
- The policy will also be displayed on the school website and

virtual learning platform.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

**Parents**

- Parents' attention will be drawn to the school eSafety Policy on the school website.