# Muschamp Primary School
# Online Safety Policy

This policy aims to set out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology
- build both an infrastructure and culture of e-Safety
- work to empower the school community to use the Internet as an essential tool for life-long learning

This policy will be used in conjunction with other school policies.

**Scope of the Policy**

This policy applies to all members of the school community (including staff, trainees, pupils, volunteers, parents, carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

**Head Teacher and Senior Leaders**

The Head Teacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead, Debbie Nicol.

- The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of the school community.

**Designated Safeguarding Lead**

The Designated Safeguarding Lead should be trained in online safety issues and:

    - will be aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying
- will take day to day responsibility for e-safety issues and will have a leading role in establishing and reviewing the school e-safety policies / documents
- will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- will liaise with the Curriculum Lead to ensure that online safety is promoted and included within PSHE lessons
- will liaise with technical staff
- will receive reports of online safety incidents

**Curriculum Lead/Technical Staff** are responsible for ensuring:

- that the school's computing infrastructure is secure and is not open to misuse or malicious attack (in accordance with Borough guidelines).
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

**Teaching and Support Staff** are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they report any suspected misuse or problem to the Head teacher, Designated Safeguarding Lead and/or Curriculum Lead for investigation / action / sanction
- digital communications with students / pupils (email / Managed Learning Environment (MLE) should be on a professional level
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor computing activity in lessons, extra curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

All staff should refer to the following government documents for information and guidance:

Teaching Online Safety in Schools
https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Education for a Connected World
https://www.gov.uk/government/publications/education-for-a-connected-world
https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

**Pupils** are responsible for using the school computing systems in accordance with the rules displayed in the computing Suite and classrooms (Appendix 1).

**Parents/Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. However, they often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). Therefore the school will take every opportunity to help parents understand and keep up to date with current issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature.

**Governors**

Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage.

The Department for Education's Keeping Children Safe in Education (2019) statutory guidance states that,

"Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools and colleges should consider this as part of providing a broad and balanced curriculum. This may include covering relevant issues through Relationships Education and Relationships and Sex Education … Personal, Social, Health and Economic (PSHE) education."

Questions that school governors should ask to help ensure their school leaders are keeping children safe online can be found at:

https://www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board

**Policy Statements**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- a planned online safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of computing and new technologies in school and outside school
- key online safety messages should be reinforced as part of a planned programme of class circle time and assemblies

- pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Keeping Children Safe in Education (KCSIE) 2025 Updates regarding online safety include adding disinformation, misinformation, and conspiracy theories to the list of content risks, providing more guidance on generative artificial intelligence (AI), and clarifying requirements for filtering and monitoring systems.

**Equipment filtering and monitoring**

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that the procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- There will be ongoing reviews of the safety and security of school computing systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted to technical staff.
- All users will have clearly defined access rights to school Computing systems
- Requests from staff for sites to be removed from the filtered list will be considered by the Head Teacher, Designated Safeguarding Lead and Curriculum Lead.
- Technical staff regularly monitor and record the activity of users on the school computing systems and users are made aware of this in the Acceptable Use Policy. Remote management tools may be used by staff to control workstations and view user activity.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Staff are not allowed to install software on the network unless authorised by Curriculum Lead.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

**Curriculum**

Online safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of computing across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the children visit.
- Children should be taught how to deal with inappropriate sites if they are stumbled upon.
- Pupils should be taught to keep themselves safe online and to be responsible in their use of different technologies

**Use of digital and video images**

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. **Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.**
- Pupils must not take, use, share, publish or distribute images of others without supervision or the permission of other pupils.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- 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 on entry to the school to allow photographs of pupils to be published e.g. on the school website

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

**E-mail**

The official school email service may be regarded as safe and secure and is monitored.

- Users need to be aware that email communications may be monitored
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**Responding to incidents of misuse**

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If members of staff or parents/careers suspect that misuse might have taken place, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In the first instance, this should involve reporting any suspicions to the Head Teacher or Designated Safeguarding Lead.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour systems in the case of pupils or disciplinary procedures in the case of staff.

Reviewed: September 2025
Review Date: September 2026

**Appendix 1**

The following rules are displayed in the Computing Suite and in classrooms where the children have access to computing equipment.

| Think before you click! |
| --- |
| e-Safety Rules |
| ● We ask permission before using the internet.<br>● We tell an adult if we see anything we are uncomfortable with.<br>● We immediately close any webpage we are not sure about.<br>● We only e-mail people an adult has approved.<br>● We send e-mails that are polite and friendly.<br>● We only print with the permission of a member of staff.<br>● We never give out personal information or passwords.<br>● We never arrange to meet anyone we don't know.<br>● We do not open e-mails sent by anyone we don't know.<br>● We do not use internet chat rooms.<br>● We do not send or reply to chain e-mails. |