# South Molton United Church of England Primary School

## E-Safety Policy

Reviewed by Teaching and Learning Committee
15th November 2022
Next Review Autumn 2023

# South Molton United C of E Primary School E-Safety Policy

This e-safety policy has been written by the school and has used the SWGFL and Government guidance to build the policy.

This policy applies to all members of South Molton C of E Primary School (including staff, pupils, volunteers, parents / carers, visitors, supply staff) who have access to and are users of school ICT systems, both in and out of South Molton United C of E Primary School.

The Education and Inspections Act 2006 empowers the Head Teacher of the School 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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.

## Purpose of this policy

The purpose of this policy is to:-

- set out the key principles expected of all members of the school at South Molton C of E Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of our School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

## What e-safety practices the school has currently in place

- The school's ICT systems will be monitored regularly and security reviewed.
- Virus protection is updated regularly
- Appropriate age related filtering is in place through internet provider and ICT Provider
- Parents are encouraged to attend e-safety training sessions run by the school.
- Parents are made aware of the E-safety and Internet Access for Pupils policy and asked to sign an acknowledgement to this effect
- Children also undertake e-safety training explaining the importance of keeping safe on the internet
- Children are encouraged to keep passwords to the schools designated learning programmes safe and not to share them with other children
- Children are asked to tell an adult if they come across something inappropriate on the internet, so it can be recorded and acted upon.

**Key Responsibilities within the school**

| Role | Responsibilities |
|---|---|
| Head Teacher | ● To take overall responsibility for e-safety provision<br>● To take overall responsibility for data and data security (SIRO)<br>● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. SWGFL<br>● To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant<br>● To be aware of procedures to be followed in the event of a serious e-safety incident.<br>● To receive regular monitoring reports from the E-Safety Co-ordinator / Officer To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures( e.g. network manager) |
| E Safety Co-ordinator | ● Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents<br>● Promotes an awareness and commitment to e-safeguarding throughout the school community<br>● Ensures that e-safety education is embedded across the curriculum<br>● liaises with school ICT technical staff<br>● To communicate regularly with SLT and the designated e-safety Governor to discuss current issues, review incident logs and filtering and change control logs<br>● To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident<br>● To ensure that an e-safety incident log is kept up to date<br>● Facilitates training and advice for all staff<br>● liaises with the Local Authority and relevant agencies<br>● Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:<br><br>• sharing of personal data<br>• access to illegal / inappropriate materials<br>• inappropriate on-line contact with adults / strangers<br>• potential or actual incidents of grooming<br>• cyber-bullying and use of social media |

| | |
|---|---|
| Governors and E-Safety Governor | ● To ensure that the school follows all current e-safety advice to keep the children and staff safe<br>● To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor<br>● To support the school in encouraging parents and the wider community to become engaged in e-safety activities<br><br>The role of the E-Safety Governor will include:<br><br>● regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs ) |
| Computing Subject Leader | ● To oversee the delivery of the e-safety element of the Computing curriculum<br>● To liaise with the e-safety coordinator regularly |
| PRAESTANTIA/School Business Manager | ● To report any e-safety related issues that arises, to the e-safety coordinator.<br>● To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed<br>● To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) To ensure the security of the school ICT system<br>● To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices<br>● the school's has age appropriate web filtering which is updated on a regular basis<br>● They keep up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.<br>● that the use of the network, remote access and email is regularly monitored in order that any attempted misuse can be reported to the E-Safety Co-ordinator or Head Teacher for investigation.<br>● To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.<br>● To keep up-to-date documentation of the school's e-security and technical procedures<br>● To be compliant with GDPR guidance in their roles as data processers and controllers.<br>● |
| School Business Manager/SCOMIS | ● To ensure that all data held on pupils on the network is adequately protected. |

| | |
|---|---|
| | ● To ensure that all data held on pupils on the school office machines have appropriate access controls in place.<br>● To be compliant with GDPR guidance in their roles as data processers and controllers. |
| Teachers | To embed e-safety issues in all aspects of the curriculum and other school activities.<br>🎬 To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities, if relevant).<br>🎬 To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. |
| All staff | ● To read, understand and help promote the school's e-safety policies and guidance<br>● To read, understand, sign and adhere to the School Staff Acceptable Use Agreement<br>● To be aware of e-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<br>● To report any suspected misuse or problem to the e-safety coordinator<br>● To maintain an awareness of current e-safety issues and guidance e.g. through CPD<br>● To model safe, responsible and professional behaviours in their own use of technology<br>● To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.<br>● To use school email addresses for school emails not personal email addresses<br>● To be compliant with GDPR guidance in their roles as data processers and controllers. |
| Pupils | ● Read, understand, sign and adhere to the Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils)<br>● Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations<br>● To understand the importance of reporting abuse, misuse or access to inappropriate materials.<br>● To know what action to take if they or someone they know feels worried or vulnerable when using online technology.<br>● To know and understand school policy on the use of mobile phones, digital cameras and hand held |

| | |
|---|---|
| | devices. To know and understand school policy on the taking / use of images and on cyber-bullying.<br>● To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.<br>● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home |
| Parents/Carers | ● To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images.<br>● To read, understand and promote the school Pupil Acceptable Use Agreement with their children.<br>● To consult with the school if they have any concerns about their children's use of technology. |
| External eg Supply Teachers | ● Any external individual /organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school. |

**Circulation**

The policy will be communicated to staff/pupils/Parents in the following ways:

- Policy to be posted on the school website/ staffroom/ school office
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year and sent to parents in starter packs
- Policy to go to Parent forum meetings
- Acceptable use agreements to be issued to external staff/volunteers, on entry to the school
- Acceptable use agreements to be held in pupil files and personnel files

**Complaints**

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

The school will take the matter very seriously and put in place steps as below:-

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by teacher / E-Safety Coordinator / Head Teacher;
- informing parents or carers;
- removal of Internet or computer access for a period;
- referral to Local authority and/or Police.

Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school and local authority child protection procedures

**Policy Review**

The E-Safety Policy relates to other school policies including child protection/safeguarding, anti-bullying, social networking and behaviour.

The School has in place a designated e-safety co-ordinator – Tom Paddon who will be responsible for monitoring e-safety within the school, reviewing the policy annually with the e-safety Governor or sooner if any significant change occurs with regard to technology use within the school.

The policy will go to SLT and Governors for final review. The school staff will all be made aware of the policy and any changes via staff meetings.

**Pupil e-safety with the curriculum**

This school:-

- Has a clear, progressive e-safety education programme as part of the Computing curriculum. It is built on e-safeguarding and e-literacy framework for Y3 to Y6 national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through our Pupil Acceptable Use Policy which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

**Staff and governor training**

This school:-

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

- Makes regular training available to staff on e-safety issues and the school's e-safety education program.

- Provide, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

**Parent awareness and training**

This school:-

Runs a rolling programme of advice, guidance and training for parents, including:

- SWGFL e-safety training for parents
- in school newsletters; on the school web site;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

**Expected Conduct and Incident management**

**Expected conduct**

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

**Incident Management**

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline, BECCA) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's SLT and Governors.
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

## 4. Managing the ICT infrastructure

### Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through Schools Broadband for web filtering;
- Has Schools Broadband block web filtering of sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature,
- Ensures network healthy through use of McAfee anti-virus software and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA approved systems such as S2S, Egress, Securnet to send personal data over the Internet and uses secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with Praestantia to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, pupils are only allowed internet access within lesson time.
- Ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the Teacher or E-Safety Co-ordinator.
- Our system administrator logs or escalates as appropriate to Schools Broadband Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

🎬 **Network management (user access, backup)**

Our school:

- Ensures the Head, SBM and SLT is up-to-date with services and policies / requires the Technical Support Provider to be up-to-date with services and policies;
- Storage of all data within the school conforms to the UK data protection requirements and is GDPR compliant.
- Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

*To ensure the network is used safely, this school:*

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also use the same username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended; Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 20 minutes and have to re-enter their username and password to re-enter the network.];
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 6 o'clock to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved suppliers.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. central stage
- Offsite backup every day for all files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;

- Ensures that all pupil level data or personal data sent over the Internet is sent within the approved secure system in our LA or through Securenet, S2S, egress ;
- Follows Praestantia Technology's advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Smartboards and Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

**Password policy**

This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;

All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private

**E-mail**

**Our school**

Provides staff with an email account for their professional use, SWGFL RM Mail and makes clear personal email should be through a separate account;

Does not publish personal e-mail addresses of staff on the school website. We use a group e-mail address, for example admin@smups.devon.sch.uk for communication with the wider public.

Will contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.

Will ensure that email accounts are maintained and up to date

Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product MCAFEE, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

**Pupils:**

At present our pupils have their own email based in school that is based on Microsoft Office to enable them to access the Office 365 Suite of Programmes.

**Staff:**

- Staff only use the schools e-mail systems for professional purposes
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; Securenet.

Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;

All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

**School website**

The Head Teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- Uploading of information is restricted to our website authorisers: Office Administrators
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address and have an enquiry form which sends to it. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

**Learning platform**

Uploading of information on the schools' Learning Platform is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;

In school, pupils are only able to upload and publish within school approved and closed systems

**Social networking**

See the school Social Networking Policy.