
# St Margaret's Anfield CE Primary School

NAME OF POLICY: E-Safety Policy

DATE: February 2021

PRODUCED BY: Mr C Feeley

**DOCUMENT STATUS**

| Version | Date | Action | Review Date |
|---|---|---|---|
| Version 1 | February 2021 | Adopted by Full Governing Body | February 2024 |
| | | | |
| | | | |
| | | | |
| | | | |

**SMA's E-Safety Policy**

## 1. Introduction and Overview

**The purpose of this policy is to:**

- Outline the guiding principles for all members of the school community regarding the use of ICT.
- Safeguard and protect the children and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations for behaviour relating to responsible use of the internet and technology for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

**Scope of the policy**

This policy applies to all members of SMA's school community; including staff, pupils, volunteers, parents and carers, visitors and all extended community users who have access to - and are users of – the school's ICT systems and digital property.

**Communication of the policy**

The policy will be communicated to the school community in the following ways:

- Displayed on the school website, and available in the staffroom and classrooms.
- Included as part of the induction pack for new staff.
- Acceptable use agreements discussed with and signed by students at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in student and personnel files.

**Responding to concerns**

- The school will take every reasonable precaution to ensure and maintain internet safety on all of its devices and digital platforms. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school, nor the Local Authority, can accept liability for material accessed, or any consequences of internet access.
- Staff and pupils are informed of the possible sanctions related to misuse of technology and these are outlined in the Behaviour Policy.
- Our E-Safety Lead, part of our wider Safeguarding team, is the first point of contact for any concerns. Any concerns about staff misuse will be referred to the Headteacher.

- Concerns that relate to online bullying will be dealt with in line with our Anti- Bullying Policy. Concerns related to child protection are dealt with in line with the SMA's child protection procedures and escalated to outside agencies if appropriate.

**Review and Monitoring**

Internet safety is integral to many other school policies; including the Computing Policy, Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

The school's E-Safety Lead is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and internet safety issues in the school.

This policy has been developed in consultation with SMA's IT & Data Manager and approved by the Senior Leadership Team and Board of Governors. Staff will be informed of any updates or amendments to it.

## 2. Education and Curriculum

**E-Safety curriculum**

The school has a clear and progressive internet safety education programme; primarily as part of the Computing curriculum but referenced in all areas of school life. The Computing curriculum has been designed alongside our partners at MGL to ensure that SMA is at the forefront of consistently delivering information and best-practice related to the ever-changing digital world. SMA also runs an e-Cadet Program where peer to peer teaching around e-safety takes place. As a school, Safer Internet Day is celebrated each year where a variety of enrichment activities covering a range of skills and behaviours appropriate to the childrens' ages and experience are provided, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The school and its partners will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind children about their responsibilities as users, ensuring the Acceptable Use Policy is signed by all.
- Ensure that staff continually model safe and responsible behaviour in their own use of technology during lessons.

- Ensure that staff and students understand issues around plagiarism and copyright, as well as intellectual and digital property rights, and understand how to assess and determine the validity of the websites they use.

**Staff and governor training**

The school will ensure that:

- Staff understand and adhere to the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information.
- Regular training is available to staff on internet safety issues and the school's e-safety education programme.
- Information and guidance on the school's Safeguarding policy and its Acceptable Use Policy is provided to all new staff – permanent and temporary - and governors as part of their induction.

**Parent engagement**

The school believes that parents and carers are vitally important in enabling and ensuring that children are able to be inquisitive online whilst remaining safe from harm and behaving responsibly. As support towards this, SMA will:

- Make its Acceptable Use Agreements available to all parents on the school's website.
- Provide regular, up to date information in newsletters and on all of its digital channels in response to emerging trends or concerns.
- Publish and promote children's learning within the field of e-safety (e.g. assemblies, performances).
- Provide support and advice on online safety to parents for when their children are outside of school.
- Share signposting to further resources and websites.

## 3. Conduct and Incident management

**Conduct**

All users are responsible for using the school ICT infastructure in line with the Acceptable Use Policy. They should understand the consequences of misuse or access to inappropriate materials.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement. They will also be given clear information about the sanctions that might result from misuse.

**Incident Management**

All members of the school community understand they have a responsibility to report issues and should be confident that anything raised will be handled quickly, sensitively, and decisively; in line with the school's policy. The school actively seeks advice and support from external agencies in handling internet safety issues. Parents and carers will be informed of any internet safety incidents relating to their own children by the practitioner responsible for e-safety or a member of the school's senior management.

## 4. Managing the ICT infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that all related policies and procedures are implemented effectively. It will also ensure that relevant staff members will be effective and diligent in carrying out their internet safety responsibilities concerning the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- All staff have individual logins and passwords.
- Where appropriate all pupils have individual logins and passwords for various learning platforms.
- The administrator passwords for the school ICT system, used by the Network Manager is also available to the Headteacher and kept in a secure place.
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school allows different filtering levels for staff than it does for children.
- The school can monitor and record the activity of users on the school technical systems and users are made aware of this.
- There is a reporting system in place for users to report any technical incident or security breach.
- Security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by robust virus software that is regularly updated.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## 5. Data

All data will be stored and handled in line with the SMA's Privacy Notice and Confidentiality Policy. These documents are available to view on the Policies page of the school's website.

## 6. Equipment and Digital Content

Expectations regarding Personal mobile phones and mobile devices are covered within SMA's Mobile Phone Policy.

### Digital images and video

All schools welcome positive publicity. Photographs of pupils can generate interest in, and bring life to, articles promoting school activities and initiatives. Making use of photographs in school publicity materials is recognised as a positive endeavour by many children and staff alike. They offer parents and carers, members of the Governing Body and the wider community an opportunity to identify and celebrate the work and achievements of the children and staff that make SMA such a welcoming and inclusive family to be a part of. A photographic record of school events can also be a useful historical record of the school's work over a long period of time. However, SMA understands that digital recordings need to be taken and used in a responsible manner.

We will seek permission from parents and carers for the use of digital photographs or video involving their child. Parents and carers are responsible for declaring, in writing, whether they refuse the school permission to publish digital recordings of their child on any of its digital platforms. Parents and carers may choose to alter their decision at any time, providing they are legally able to do so, by providing written confirmation in the form of a signed letter or email.

Children are all taught to think extremely carefully about placing any personal photos on social media platforms. The importance of privacy settings as a tool to safeguard their personal information, as well as the importance of valuing the ownership of their digital property, is included in internet safety education. They are also taught that they should not post images or videos of others without consent from responsible adults.

Children are clearly explained and understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school. They are encouraged to exhibit responsible caution at all times when online.