Believe and Achieve Together

St Mary's CE Primary School

Online Safety Policy

Adopted:	January 2019
Review:	January 2023
Next Review:	January 2026

"I pray that you would be rooted and established in love…..
Filled to the measure of the fullness of God" (Ephesians 3:17-19)

Introduction

The Governing Body of St Mary's CE Primary School want all members of our school community to enjoy and benefit from the advantages that technology offers for learning. We do not want the inherent risks associated with access to information, electronic communications and social networking to reduce our use of technology. Instead we want to ensure that our staff, pupils and Governors use the internet in a responsible way so that they do not put themselves or others at risk.

Purpose

The purpose of the online safety policy is to:

- Promote the use of technology within the curriculum.

- Protect children from harm.

- Ensure that the school fulfils its duty of care to pupils.

- Provide clear expectations for staff and pupils on acceptable use of the internet.

At St Mary's we will do this by: -

- Providing a safe internet platform using Senso, which will minimise the chances of pupils encountering unsuitable material.

- Developing a culture of safe practice where everyone is aware of the expected standards of online behaviour.

- Giving staff training a high priority.

- Teaching our children to keep themselves and others safe online and use technology responsibly.

- Ensuring online safety is embedded in the curriculum and actively promoted and a high profile is maintained.

- Working in partnership with parents and carers to raise awareness of the potential risks of internet use.

- Ensuring all internet users sign an Acceptable Use Agreement that sets out their rights and responsibilities and incorporates the school's online safety rules.

This policy must be read in conjunction with our "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".

Roles and Responsibilities

Every member of the school community has a role to play in online safety.

Headteacher

The Headteacher has ultimate responsibility for online safety issues including:

- The development, implementation and review of the school's online safety policy.

- Ensuring that online safety issues are given a high profile within the school community.

- Linking with the Governing Body and parents and carers to promote online safety.

- Ensuring online safety is embedded in the curriculum.

- Ensuring that staff and pupils are aware that any online incident should be reported to them.

- Being the first point of contact and advice for school staff, Governors, pupils and parents.

- Keeping up to date with online safety issues and advise of new trends, incidents or arising problems, including assessing the impact of emerging technology and the school's response to this.

- Managing sanctions against staff and pupils who are in breach of the Acceptable Use Agreement.

- Raising the profile of online safety awareness by ensuring regular staff and governor training.

- Ensuring all staff, pupils and Governors have read and signed the Acceptable Use Agreement.

- Liaising with ICT support to ensure that the anti-virus and filtering systems are maintained, audits are carried out and any breaches investigated and records kept.

School Staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is to:

- Adhere to the school's online policy and acceptable use procedures (see "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".)

- Communicate the school's online policy and acceptable use procedures to pupils.

- Engage in online safety training.

- Keep pupils safe and ensure they receive appropriate supervision and support whilst using the internet.

- Plan use of the internet for lessons and researching online materials and resources.

- Report breaches of internet use to the Head Teacher.

- Recognise when pupils are at risk from their internet use or have had negative experiences and take appropriate action. Examples of risk might be inappropriate contact with an adult they have met online; risk from contact with violent extremists; risks from sites advocating suicide, self-harm and anorexia.

- Ensure online safety awareness is embedded in all teaching of PSHE, Computing and other lessons where IT is used so that pupils have the opportunity to discuss issues affecting them in an open and safe environment.

- Be able to access pupil's emails and other internet files generated in school and check these periodically to ensure that expectations of behaviour are being met

- Be aware of those children with special needs or those who may be more vulnerable to risk from internet use (generally those children with a high level of experience and good computer skills coupled with poor social skills).

Parents and Carers

The school recognises that most children will have internet access at home or on their own mobile devices and might not be as closely supervised as they would be at school. Children may be put at risk in the following ways:

- By being exposed to inappropriate content e.g. pornography or information advocating violence, suicide or illegal behaviour.

- By having inappropriate contact e.g. through chat rooms, gaming sites, disclosing own personal information or images or cyber bullying.

- By being enticed or persuaded to provide sensitive or private financial information putting themselves or others at risk of unregulated or illegal commercial activity.

The school will work with parents and carers to promote that online safety messages are reinforced at home. We strongly believe that limiting or denying a child access to the internet will not ultimately protect them from the inherent risks. Ultimately we want children to take responsibility for their own choices by understanding the risks and being able to explore online safety issues in the relatively 'safe' environment of school.

The school will:

- Provide parents/carers with online safety updates.

- Signpost parents/carers to useful resources.

- Alert parents/carers to online safety concerns as they arise (e.g. relating to particular incidents, apps etc).

Each September we ask parents/carers to agree or not agree to visual media of their children being included on the school website and other online platforms that the school uses.

Further information can be found in "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".

Pupils

- All pupils are expected to read and agree the Acceptable Use Agreement for Pupils annually having discussed it first with their teachers and parents/carers.

- Pupils are taught to take responsibility for their own behaviour and this includes the material they choose to access on the internet and the content of any online communications.

- Pupils are taught that should they encounter an unsuitable site or be unhappy about any online communications they should alert a member of staff.

<u>Using the Internet in the Classroom</u>

- Teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Pupils should not be allowed to aimlessly 'surf' the internet and all use should have a clearly defined educational purpose.

- When using the internet children should receive an appropriate level of supervision for their age and understanding.

- Computers / tablets should not be used at break times.

- YouTube is a valuable resource but should be used with caution. Children should not search it without close supervision.

- Social Networking Sites, Chat Rooms, Messaging and Gaming Sites are not accessible via the school's network.

- If a teacher or pupil unintentionally opens a website with content that is upsetting or inappropriate they should immediately minimise the window. Staff should reassure the pupil they have done nothing wrong and reinforce the online safety message. The incident should be reported to the Head Teacher and the URL and website provided so that the site can be blocked for the future.

Teaching Online Safety

Pupils are taught all elements of online safety included in the PSHE and Computing curricula including but not limited to:

- Keeping personal information private e.g. not to give out personal details to anyone online that may help to identify or locate them or anyone else for example home address, name of school or clubs identified.

- Only using moderated chat rooms that require registration and are specifically for their age group.

- Not uploading personal photos of themselves or others onto sites and to take care regarding what information is posted online as there is no control of who sees images.

- Setting up security and privacy settings on sites.

- Behaving responsibly whilst online and keep communications polite.

- Not responding to any hurtful or distressful messages but to let their parents, carers or teachers know so action can be taken.

- Not arranging to meet anyone whom they have only met online or go offline with anyone they meet in a chat room.

- Identifying where to go for help and support when they have concerns about content or contact on the internet or other online technologies In this way they can become responsible, confident, competent and creative users of information and communication technology.

Personal IT Devices (Pupils)

Pupils are allowed to bring a mobile phone with them to school but this must be handed into the school office when arriving on site and collected when leaving. Pupils are not allowed to used phones or other devices during the school day, or whilst attending after school activities, unless for medical reasons.

Information relating to staff use of personal IT devices can be found in "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".

Potential Abuse of the Internet

Intentional access of inappropriate websites by a pupil

If a pupil deliberately accesses inappropriate or banned websites they will be in breach of the Acceptable Use Agreement. The incident should be reported to the Head Teacher who will decide an appropriate course of action.

Inappropriate use of IT by staff or Governors

If a member of staff witnesses misuse of IT by a colleague they should report this immediately to the Headteacher or Chair of Governors. This school's disciplinary procedure will be invoked and followed.

See "Policy for the Acceptable Use of the Computer System and Social Media (Staff)".

Cyberbullying

Cyberbullying is defined as the use of technology such as email, messaging and social networking sites to deliberately hurt, upset, harass or threaten someone. The internet allows this form of bullying to continue past school hours and invades the victim's home and personal life. It can affect pupils and staff members.

Bullying may take the form of:

- Rude, abusive or threatening messages via email or text

- Posting insulting, derogatory or defamatory statements on blogs or social networking sites

- Setting up web sites that specifically target the victim

- Making or sharing derogatory or embarrassing images or videos of someone via mobile phones or email.

In extreme cases cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

The key points to note are as follows:

1. Any incidents of cyber bullying should be reported to the Headteacher. These will be dealt with in line with our behaviour or anti-bullying policies.

2. Extreme incidents will be reported to the Police.

3. Pupils will be taught

   - To only give out mobile phone numbers and email addresses to people they trust

   - To only allow close friends whom they trust to have access to their social networking page. Please note that most social networking sites have a minimum age of 13 and as such children and parents will be advised not to have these for primary age children.

   - Not to send or post inappropriate images of themselves

   - Not to respond to offensive, upsetting or hurtful messages

   - To report any problems or worries to their parents and teacher immediately. Cyber bulling of employees It is entirely possible that employees at the school may themselves become victims of cyberbullying either by pupils or parents. Further details and advice for employees should be sought from the Head Teacher.