SS Mary and John's Online Safety Policy

Governing Body Date Approved	**January 2025**
Category Recommended	**DfE**
Next Review Date Every two years unless a change in legislation	**January 2027**
Policy Availability	**Available on the school website.**
Officer Responsible	

Contents

1. Scope

This policy applies to all members of the SS Mary and John Catholic Primary School (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school integrated technologies both in and out of school sites. **Technologies for the purposes of this policy refers to, but is not limited to, devices, systems, and the internet. **

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for academies on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Equality Act 2010, and the Education Act 2011.

The Education and Inspections Act 2006 empowers Principals 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 online-bullying or other online 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 which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

2. Aims

Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and SSMJ/Trust Board. Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

3. Roles and responsibilities

3.1 The Trust Board

The Governing Body has the overall responsibility for monitoring this policy and holding the Principal to account for its implementation. The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the DSL/Deputy DSL(s). All members of the Governing Body will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms of acceptable use of school technologies and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing the approach to safeguarding and related policies

3.2 The Principal and Senior Leaders

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety may be delegated to another senior member of school staff or those responsible for safeguarding.
- The Principal and (at least) 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 staff.
- The Principal / Senior Leaders are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

3.3 The Designated Safeguarding Lead

*In some instances, the DSL may be the school Principal. Details of the school's designated safeguarding lead (DSL) and deputy are set out in the Child Protection and Safeguarding Policy and on the school website

The DSL/Deputy DSL(s) takes lead responsibility for online safety in the school, in particular:

- ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with staff, as necessary, to address any online safety issues or incidents
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Primary Anti-Bullying Policy
- updating and delivering staff training on online safety, liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in the school to the Principal and/or Standards and Performance Committee

This list is not intended to be exhaustive. The DSL/Deputy DSL(s) should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding 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
- online-bullying

3.4 All Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current Online Safety Policy and practices
- they have read, understood, signed, and adhere to the Staff Acceptable Use Agreement (AUA)
- they report any suspected misuse or problem to the Principal or appropriate Senior Leader and/or the DSL/Deputy DSL(s) for investigation / action / sanction and logging on the appropriate systems.

- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use agreements
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies (such as mobile devices, cameras, etc.) in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use, processes should be in place for dealing with any unsuitable material that is found in internet searches. Teachers when planning to use the internet as part of lessons will give consideration to a pupils age and stage
- Online safety incidents are logged and dealt with appropriately in line with this policy
- Incidents of cyber-bullying are dealt with appropriately in line with the Primary Anti-Bullying Policy

3.5 Technical Support

Technical Support is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at the school, including terrorist and extremist material
- Ensuring that the school's technical systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's technical systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
-

This list is not intended to be exhaustive.

3.6 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. The school will take every opportunity to help parents understand these issues. Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms of acceptable use of school technologies and the internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: What are the issues? - UK Safer Internet Centre
- Hot topics, Childnet International: Help & advice | Childnet
- General parental information: Parents and carers | CEOP Education (thinkuknow.co.uk)

3.7 Pupils

* Application of the Online Safety Policy relating to the responsibilities of pupils should always be applied appropriate to the age and stage of the pupils Pupils:

- are responsible for using school technologies in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Primary Online Safety Policy covers their actions out of school, if related to their membership of the school

3.8 Visitors and members of the community

Visitors and members of the community who use school technologies will be made aware of this policy, when relevant, and are expected to read and follow it. They will be expected to agree to the terms of acceptable use and must sign the Staff /Volunteers Acceptable Use Agreement

4. Educating pupils about online safety

Pupils will be taught about online safety both as part of the Computing curriculum and as part of RSE\PSHE lessons; there is a strong link between the learning objectives related to online safety with many of the online safety lessons aligning with RSE\PSHE objectives.
Additionally, online safety will be covered in each year group with objectives building upon those taught in previous years in order to better enhance the digital literacy of our pupils.

Year 1

	Unit 1.1	Unit 1.2	Unit 1.3	Unit 1.4	Unit 1.5	Unit 1.6	Unit 1.7	Unit 1.8	Unit 1.9
	Online Safety & Exploring Purple Mash	Grouping & Sorting	Pictograms	Lego Builders	Maze Explorers	Animated Story Books	Coding	Spreadsheets	Technology outside school
Number of lessons	4	2	3	3	3	5	6	3	2
Main tool			2Count		2Go	2Create A Story	2Code	2Calculate	

Year 2

	Unit 2.1	Unit 2.2	Unit 2.3	Unit 2.4	Unit 2.5	Unit 2.6	Unit 2.7	Unit 2.8
	Coding	Online Safety	Spreadsheets	Questioning	Effective Searching	Creating Pictures	Making Music	Presenting Ideas
Number of lessons	6	3	4	5	3	5	3	4
Main tool	2Code		2Calculate	2Question 2Investigate		2Paint A Picture	2Sequence	

Year 3

	Unit 3.1	Unit 3.2	Unit 3.3	Unit 3.4	Unit 3.5	Unit 3.6	Unit 3.7	Unit 3.8	Unit 3.9
	Coding	Online safety	Spreadsheets	Touch Typing	Email (inc. email safety)	Branching Databases	Simulations	Graphing	Presenting
Number of lessons	6	3	3 4 lessons for Crash Course	4	6	4	3	2	5\6*
Main tool	2Code		2Calculate	2Type	2Email	2Question	2Simulate	2Graph	PowerPoint or Google Slides

*Platform dependent

Year 4

	Unit 4.1	Unit 4.2	Unit 4.3	Unit 4.4	Unit 4.5	Unit 4.6	Unit 4.7	Unit 4.8	Unit 4.9	Unit 4.10
	Coding	Online Safety	Spreadsheets	Writing for Different Audiences	Logo	Animation	Effective Searching	Hardware Investigators	Making Music	(Optional Unit) Introducing AI
Number of lessons	6	4	6	5	4	3	3	2	4	4
Main tool	2Code		2Calculate		2Logo	2Animate			Busy Beats	

Year 5

	Unit 5.1	Unit 5.2	Unit 5.3	Unit 5.4	Unit 5.5	Unit 5.6	Unit 5.7	Unit 5.8	Unit 5.9
	Coding	Online Safety	Spreadsheets	Databases	Game Creator	3D Modelling	Concept Maps	Word Processing	External Devices
Number of lessons	6	3	6	4	5	4	4	8	6
Main tool	2Code		2Calculate	2Investigate	2DIY 3D	2Design & Make	2Connect	MS Word or Google Docs	2Code Purple Chip

Year 6

	Unit 6.1	Unit 6.2	Unit 6.3	Unit 6.4	Unit 6.5	Unit 6.6	Unit 6.7	Unit 6.8	6.9
	Coding	Online Safety	Spreadsheets	Blogging	Text Adventures	Networks	Quizzing	Understanding Binary	Spreadsheets
Number of lessons	6	2	5	4	5	3	6	4	8
Main tool	2Code		2Calculate	2Blog			2Quiz		Excel or Google Sheets

4.1 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their groups, and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Trustees, Governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
In relation to a specific incident of cyber-bullying, the school will follow the steps set out in the Trust's Anti-Bullying Policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

5. Educating parents/families about online safety

SSMJ will share this policy with parents/families to raise awareness of internet safety. The following information will be communicated to parents/families:

- What systems are being used in the school to filter and monitor online use
- What children are being asked to do online (e.g., sites they need to visit or who they will be interacting with online)

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL/ Deputy DSL.

6. Acceptable use

All pupils, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of school technologies and the internet. Visitors will be expected to read and agree to the school's terms of acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

7. Mobile devices in school

Pupils are not permitted to bring mobile devices into the school. Mobile devices brought into school should be confiscated and returned to the pupils' parent/carer. With the exception of Year 6 pupils who are walking home. In this instance mobile devices will be held at the office until the end of the day before being returned to pupils.
Staff are permitted to bring mobile devices into the school but are not permitted to use their mobile devices around pupils and their families.

8. Staff using work devices outside school

Staff members using a work device outside of the school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work

device when using it outside school. USB devices containing data relating to the school are not permitted.
If staff have any concerns over the security of their device, they must seek advice from technical support staff. Work devices must be used solely for work activities.

9. How the school will respond to issues of misuse

Where a pupil misuses school technologies or the internet, we will follow the guidance set out in the Primary Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses school technologies or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
The DSL and Deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in each school's Child Protection and Safeguarding Policy.

11. Monitoring arrangements

The DSL/Deputy DSL logs behaviour and safeguarding issues related to online safety.
This policy will be reviewed by SSMJ Board of Governors and the DSL/ Deputy DSL as per the frequency stated on the front cover. At every review, the policy will be shared and approved by the governors

Appendix One: Acceptable Use Agreement for staff, volunteers, and visitors.

Acceptable use of the school technologies including devices, systems and the internet: agreement for staff, volunteers and visitors.

Name:

Staff / Volunteer / Visitor Acceptable Use Agreement

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within the School and in their lives outside the School. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

• Staff, volunteers and visitors will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
• School technologies (including, but not limited to, devices and systems) and users are protected from accidental and / or deliberate misuse that could put the security of the systems or safety of users at risk.
• Staff are protected from potential risk in their use of technology in their everyday work.

The School will try to ensure that staff and volunteers will have good access to technology to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use technology in a responsible way, to ensure that there is no risk to my safety or to the safety and security of other users and / or school technologies. I recognise the value of the use of technology for enhancing teaching and learning, creating efficiencies and reducing workload, and will ensure that pupils receive opportunities to gain from the use of technology. I will, wherever possible, educate the young people in my care in the safe use of technology and embed online safety in all aspects of my work with young people. I will have an up-to-date awareness of online safety matters and of the current Primary Online Safety Policy and practices.

For my professional and personal safety:

• I understand that the school will monitor my use of technology, including, but not limited to, the monitoring of digital communications including email, the use of school devices and the use of the internet on school devices and systems (i.e. school internet connections etc) using software such as Smoothwall.
• I understand that the rules set out in this agreement apply to the use of all school technologies including, but not limited to, devices and systems i.e. laptops, iPads, gmail, Google Drive etc…) both inside and outside of the school.

• I understand that all technology within the school is intended for educational use or the operations of the school.
• I will not disclose any of my usernames or passwords to anyone else, nor will I try to use any other person's username and password.
• I will immediately report any illegal, inappropriate or harmful material or incident I become aware of.
• I will report any suspected misuse for investigation / action / sanction and ensure that incidents are logged in accordance with the appropriate school policies**.**

I will be professional in my communications and actions when using school systems:

• I will not access, copy, remove or otherwise alter any other user's files, without permission, unless shared for the purpose of collaboration or in the spirit of reducing workload.
• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with all relevant Trust, Phase or Local policies I will not use my personal equipment to record images, unless I have permission to do so. Where these images are published, it will not be possible to identify by name, or other personal information, those who are featured.
• I will not use social media sites/apps within the school unless prior approval has been granted and use is in line with my role.
• I will only communicate with pupils / parents / carers using official school systems. Any such communication will be professional in tone and manner.
• I will not share any personal information with a pupil.
• I will not communicate with any current pupils digitally other than through PurpleMash. Any such communications will be professional in nature and in line with my role.
• I will not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of the professional role.
• I will ensure that all communications are transparent and open to scrutiny.
• I will not give out my personal contact details to pupils, including, but not limited to, my mobile telephone number, personal email addresses, social media profiles and details of any blogs/vlogs or personal websites/channels.
• I will not accept or invite pupils as 'friends' on social media sites or apps and must delete any of these young people currently accepted as 'friends' on any social media sites or apps.
• I will review 'friend lists' regularly and remove any current pupils or person under the age of 18 years where it could be perceived as inappropriate to maintain contact with that young person.
• I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and to ensure the smooth running of the school:
• I will not connect personal devices to school systems.
• I will not use storage devices to store and/or transport sensitive documents including those containing pupil data or information.
• I will avoid the use of USB sticks where possible opting to use OneDrive or O365 in order to access files.
• I will not open any attachments to online communications such as emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
• I will ensure that my data and files on school devices are regularly backed up, in accordance with relevant school policies. I will endeavour to use OneDrive to store files avoiding the need for files or data to be stored on the device.
• I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others (child sexual abuse images, criminally racist material, adult

pornography). I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
• I will not install or attempt to install programmes or software of any type on a machine, or store programmes or software on a computer, nor will I try to alter computer settings.
• I will not disable or cause any damage to school equipment, or the equipment belonging to others.
• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Data Protection Policy. Any transferring of data outside of the school will be in line with the Trust Data Protection Policy.
• I understand that the Trust Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the Trust Data Protection Policy to disclose such information to an appropriate authority.
• I will immediately report any damage or faults involving equipment or software, however this may have happened, regardless of fault.

When using the internet in my professional capacity or for school sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work
• Where work is protected by copyright, I will not download or distribute copies (including music, images and videos).

I understand that I am responsible for my actions in and out of the school:

• I understand that this Acceptable Use Agreement applies not only to my work and use of school technologies in the school, but also applies to my use of school technologies outside of the school and my use of personal equipment in the school or in situations related to my employment by the school.
• I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use school technologies (both inside and outside of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:	
Signed:	
Date:	