

ACCEPTABLE USE AND E-SAFETY POLICY

**Acceptable Use and
E-Safety Policy
for
St Mary's C.E. Primary School**

Approved by the Governing Body:	February 2023
Date of next review:	February 2026

Acceptable Use and E-Safety Policy

This policy has been written to provide a guide to acceptable use of the Internet at St Mary's CE Primary School.

1 INTRODUCTION

The internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the internet make it an invaluable resource for all to use on a daily basis. However, some of the material is published for adult audiences and is unsuitable for pupils. E-mail and chat communication via social media can also be used inappropriately and therefore it is a necessity to provide our pupils with protection from inappropriate material or communications.

2 THE IMPORTANCE OF THE INTERNET IN SCHOOL

The purpose of using the internet in school is to raise educational standards, to expose pupils to the use of this vital resource and learn how to navigate it effectively and safely, to support the professional work of staff and to enhance the school's management information and business administration systems.

Using the internet is part of the statutory curriculum and a necessary tool for staff and pupils.

The internet has enormous potential to enhance the learning process. To the world of education, the development of the internet is the most significant advance in technology since the invention of printing. Its potential to unlock new ways of teaching and learning is immeasurable.

3 HOW THE INTERNET BENEFITS EDUCATION

Benefits of using the internet in education include:

- Educational and cultural exchanges between pupils worldwide.
- Contributes to raising standards by giving pupils access to knowledge beyond that which is immediately available in the classroom.
- Inclusion in government initiatives such as the London Grid for Learning.
- Professional development for staff through access to national developments, educational materials and good curriculum practice.
- Communications with support services, professional associations and colleagues within and outside the borough.
- Exchange of curriculum and administration data with the local education authority (LA) and Department for Education (DFE).
- Improved access to technical support including remote management of networks.
- Access to worldwide educational resources including museums and art galleries.

4 ENSURING INTERNET ACCESS IS APPROPRIATE AND SAFE

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

Pupils in school are unlikely to see inappropriate content in books because publishers, teachers and other education staff select books carefully. Similarly, we take the following key measures to help ensure that our pupils are not exposed to unsuitable material via the internet:

- Our internet access is provided by the London Grid for Learning (LGfL), which provides a service designed for pupils, including a filtering system. The filter is currently set at the 'severe' rating to provide the highest possible protection.
- Pupils using the internet are normally working in classrooms, during lesson time, and are supervised by an adult (usually the teacher) at all times.
- Staff check that the sites pre-selected for pupil use are appropriate to their age and maturity.
- Staff are particularly vigilant when pupils are undertaking their own searches and check that they follow the agreed search plan.
- Pupils are taught to use e-mail and the internet responsibly, in order to reduce the risk to themselves and others.
- The Computing Lead monitors the effectiveness of internet access strategies
- The Headteacher ensures that the policy is implemented effectively and this is monitored by governors through the curriculum committee and safeguarding governor.
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material are reviewed in consultation with colleagues from other schools and advice from the Local Authority (LA), our Internet Service Provider (Adept) and the Department for Education.
- Staff are vigilant about the content of e-mail and web pages.
- Pupils sign a class contract 'Pupil user Agreement' that states that they will use the internet safely. See Appendix 1.

5 WHAT HAPPENS IF PUPILS ENCOUNTER INAPPROPRIATE MATERIAL?

Despite these precautions, the scale of the internet, the fact that it is international and that much of the material is linked mean that it is not possible to guarantee that any particular type of material will never appear on a computer screen. Neither the school

nor the London Borough of Richmond upon Thames can accept liability for the material accessed, or any consequences thereof.

One of the most important elements of our rules of responsible internet use is that pupils be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable or is inappropriate. If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will respond to the situation quickly and on a number of levels. All breaches of the e-safety policy are recorded and forwarded to the Safeguarding Lead. The details of the user, date and incident are reported and evidence of incidents is preserved and retained.

Responsibility for handling incidents involving pupils will be taken by the responsible adult (usually the class teacher), the Computing Lead and the Senior Leadership Team – appendix 3 is used to support staff in how to respond. All teaching staff will be made aware of the incident at a staff meeting if appropriate. In all circumstances, an e-safety incident will be logged by the class teacher and passed on to the Computing Lead. See appendix 2 for an e-safety incident recording form.

If one or more pupils discover (view) inappropriate material, our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and explained the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issues.

If any staff or pupil discovers unsuitable sites, the Computing Lead will be informed. The Computing Lead will report the web address and its content to the school's Internet Service Provider, Adept, and to the LA. The site will be immediately blocked to all Richmond schools and a firewall put in place.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Safeguarding Leads immediately – it is their responsibility to decide on appropriate action not the class teachers.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the rules of responsible internet use. Pupils who abuse the privileges of internet and e-mail access by failing to follow the rules they have been taught or failing to follow the agreed search plan will have sanctions applied. See also the anti-bullying policy regarding inappropriate use of email and social media.

6 MAINTAINING THE SECURITY OF THE SCHOOL'S ICT NETWORK

Connection to the internet significantly increases the risk that any computer or network is infected by a virus or accessed by unauthorised persons. The school subscribes to Sophos anti-virus protection plan provided through LGFL where an up-to-date scan takes place to ensure system security from latest viruses or any information that may harm our network.

7 USING THE INTERNET TO ENHANCE LEARNING

Staff and pupils learn how to use web browsers, search engines and find and evaluate information via the internet. Access to the internet is part of planned curriculum time that enriches and extends the learning activities integrated into our schemes of work.

As in other areas of work, we recognise that pupils learn most effectively when given clear objectives. Internet access is designed expressly for pupil use and includes a filtering service provided by Adept.

Pupils use different ways of accessing the internet depending upon their age and the nature of material required:

- Access to the internet may be demonstrated by the teacher (or sometimes other adults).
- Pupils may access teacher prepared materials, rather than the open internet.
- Pupils may be directed to a specific web page or site to use.
- Pupils may be provided with a list of relevant and suitable sites which they may access.
- Older, more experienced pupils may be allowed to undertake their own internet search having agreed a search plan with their teacher. Pupils will be expected to observe the rules of responsible internet use and will be informed that checks can and will be made on files held on the system and the sites accessed.

Pupils accessing the internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the pupils' minds as they monitor the use of the internet.

8 USING INFORMATION FROM THE INTERNET

To use information from the internet effectively, it is important for pupils to develop an understanding of the nature of the internet and the information available on it. In particular, they should know that, unlike the school library, for example, most of the information on the internet is intended for an adult audience, much of it is not properly audited/edited and most of it is copyright. Therefore:

- Pupils are taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV.
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet.
- When copying materials from the web, pupils are taught to observe copyright laws.
- Pupils are made aware that the writer of an e-mail or an author of a web page may not be the person claimed.
- Pupils will not be permitted access to any public or unregulated chat rooms for any reason.

9 USING E-MAIL

Pupils learn how to use an e-mail application and are taught e-mail conventions. Staff are registered with the London Borough of Richmond and all have an allocated e-mail address.

It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- Pupils do not have their own email addresses through the school the London Grid for Learning. Pupils send e-mails as part of planned lessons through a software program that the teacher has authority over, but do not receive individual e-mail accounts.
- Pupils are not permitted to use personal e-mails at school to arrange to meet someone outside school hours.
- Please see anti-bullying policy regarding the school's policy on handling cyber-bullying.

10 ST MARY'S WEBSITE, TWITTER AND BLOGS

Our school website, Twitter and blogs are intended to provide accurate, up to date information about our school. They enable pupils to publish work to a high standard, for a wide audience including pupils, parents, staff, governors, members of the local community and others. It is a way of celebrating pupils' work and providing them with the opportunity to publish their work on the internet as well as promote the school.

All classes may provide work for publication on the school website and Twitter. Class teachers are responsible for ensuring that the content is accurate and the quality of presentation is maintained. The web manager is responsible for ensuring that pages are up-loaded to the school site regularly, that the links work and that the site meets the requirements of the host.

The point of contact on the website is the school's address, telephone number and e-mail address. We do not publish pupils' full names or photographs accompanied by names that identify individuals on our web pages. Home information or individual e-mail addresses will not be available either.

11 E-SAFETY USING PORTABLE EQUIPMENT

The school does not permit pupils to bring their own electronic equipment into school (including digital cameras, music players); however, in Years 5 and 6, when pupils walk home alone, they can bring in their mobile phone. This is as a safety precaution. Any such items must be kept securely with the class teacher during school hours and returned to the pupil at the end of the school day. All mobile phones are brought into school and left at the owner's risk.

Staff are required to ensure that any portable equipment they may bring into school – PDAs, mobile phones, laptops, music players etc - are kept secure and that pupils cannot access them. Any such item found with inappropriate material will invoke disciplinary measures (see Staff Disciplinary Procedures). The school's Safeguarding Policy states that staff should always delete any images of pupils from their personal devices (e.g. phone), taken for work purposes, before leaving school premises each day.

There may be occasions when pupils are issued with portable electronic equipment by the school for certain projects and exercises e.g. digital cameras, video cameras, dictaphones. Where possible, the use of this equipment will be supervised by a member of staff; however, all pupils will be taught the correct, safe and appropriate use of such equipment and made aware what is deemed to be inappropriate and the consequences.

12 E-SAFETY IN THE CURRICULUM

E-safety forms part of the National Curriculum for computing. The Computing Lead ensures that each year group learns e-safety skills and knowledge appropriate to their age group and exposure to the internet. The school's computing scheme of work is supplemented by additional e-safety learning and resources to meet these aims. The Computing Lead is responsible for keeping abreast of developments in the digital world that may affect pupils. Pupils are taught where and when to show caution when online and, importantly, what to do if they are unsure: report it to a trusted adult. The school takes part in Safer Internet Day each year ensuring the profile of e-safety remains high at St Mary's.

Pupils learn about the challenges of using social media and how to be responsible digital citizens when using such forums, both in the Computing and PSHE curriculum. Pupils are taught how to respond if they witness inappropriate behaviour on social media or online: reporting it to a trusted adult. Whilst the use of social media will take place exclusively away from school and out of school hours, the school will act on inappropriate behaviour, in conjunction with parents/carers (see anti bullying policy), if brought to its attention.

School staff regularly receive e-safety training.

13 E-SAFETY FOR PARENTS

The school supports parents in keeping children safe when using technology and the internet. The school encourages all parents and carers to download the Safer Schools app which keeps parents abreast of the latest e-safety developments. The school reminds parents that social media apps and websites have age restrictions – in most cases 13+ years old and some older – and are not appropriate for primary school children. Parents are supported in keeping children safe online at home in setting up parental restrictions on popular devices.

Parents are regularly invited to parent e-safety training.

14 EQUALITIES STATEMENT

St Mary's positively celebrates diversity and inclusion is core to its Christian ethos. The Governing Body recognises that no one should receive less favourable unlawful treatment than another on the grounds of gender, marital or civil partnership status, colour, race, nationality, ethnic or national origin, disability, religious beliefs, age, or sexual orientation. It is the Governors' aim that no-one at the School should suffer unlawful direct or indirect discrimination, victimisation or harassment on any of these grounds. The Governing Body is committed to embedding fairness and equality at the heart of the school community, and in all aspects of the school's policies, procedures and practices.

15 LEGAL FRAMEWORKS

Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be technical challenge, data theft or to damage the system or data.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the rights for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic

monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.

Data Protection Act 1984/98 concerns data on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software

Telecommunications Act 1984 Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system

Protection of Children Act 1978


Obscene Publications Act 1959 and 1964 defines "obscene" and related offences

APPENDIX ONE

Key Stage 1 Class Contract

Pupil Contract: Acceptable Use Agreement 2022-23

Read the statements and tick each box.

I keep SAFE online because ...	
I CHECK it's OK to use a website/game/app.	
I ASK for help if I get lost online.	
I THINK before I click on things.	
I KNOW online people are really strangers.	
I am RESPONSIBLE so never share private information.	
I am KIND and polite online.	
I TELL a trusted adult if I am worried about anything.	

Class: _____

Name: _____

Date: _____

Key Stage 2 Class Contract

Pupil Contract: Acceptable Use Agreement 2022-23

This agreement will help keep me safe and help me to be fair to others.

- *I am an online digital learner* - I use the school's IT (Chromebooks, IPADS and Computers) for schoolwork, homework and other activities approved by trusted adults.
- *I am careful online* - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- *I am guarded online* - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- *I am cautious online* - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- *I am considerate online* - I do not get involved with bullying or sharing inappropriate material.
- *I am respectful online* - I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.
- *I am responsible online* - I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.
- *I am a creative digital learner online* - I only edit or delete my own digital work and only use other people's work with their

permission or where the work is shared through a Creative Commons licence.

- *I am a researcher online* - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- *I communicate and collaborate online* - with people I know and have met in real life or that a trusted adult has approved.
- *I am SMART online* - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.
-

Sign your name below to state you agree with your class contract.

Class: _____ Name: _____

_____ Date: _____

APPENDIX TWO

E-Safety incident reporting pro-forma

Name of adult investigating the incident _____

Name of adult or young person reporting the incident _____

Date of incident _____

Where and when did it take place? _____

Name(s) of person involved in the incident _____

Summary of incident

What action has been taken and have parents or carers been involved?

State any sanctions or actions involving perpetrator(s)

State any support that has been offered to those involved

Has the incident been resolved to the satisfaction of the e-safety officer?
Yes / No / Still being investigated (please comment below, if appropriate)

APPENDIX THREE

Online safety incident Procedure Flow Chart

