Online Safety Policy

Policy updated: October 2026

To be reviewed: October 2027

This policy should be read in conjunction with the following:

- ICT Acceptable Use policy
- Mobile Phone policy
- Behaviour policy
- Safeguarding policy
- PSHE and RHE policy
- Reasonable use of AI policy

Our School Vision

We are distinctively Christian in our ethos and outlook and are inclusive of all. At the heart of our school are our Christian values. We welcome those of all faiths and none to shine their lights brightly, and celebrate joys, failures and successes in partnership with parents and the community

Kindness Forgiveness Fairness Hope Courage Respect

1. Introduction

The Internet and digital technologies are essential resources to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology. In delivering the curriculum, teachers must plan for the integration of communications technology such as web-based resources, e-mail, and cloud-based learning platforms. Computing skills are vital for lifelong learning and employment; indeed, computing and the use of digital technology are now essential life skills. In line with KCSIE 2026, this policy also recognises the need to educate pupils about emerging technologies, including artificial intelligence (AI), misinformation, disinformation, and harmful online narratives.

Pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. Young people have access to the Internet from many places including home, school, friends' homes, libraries and in some cases mobile phones. St Peter and St Paul C of E Primary School has a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. St Peter and St Paul C of E Primary School is therefore ideally placed to help its pupils to learn how to become e-safe. We want to equip our pupils with the knowledge needed to make the best use of the Internet and digital technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

2. Aims

At St Peter and St Paul C of E Primary School, we aim to provide a safe and engaging learning environment where children can achieve their full potential. Access to the Internet is a powerful tool that enhances learning opportunities and teaching practice.

We believe that access to the Internet will:

- Enrich the quality of curriculum provision and extend learning activities
- Raise children's attainment
- Support teachers' planning and resourcing of lessons
- Enhance the school's management and administration systems
- Support professional development through access to educational materials and network
- 3. Filtering, Monitoring and Cybersecurity

Our school uses RM Safetynet Go - DfE-approved filtering to prevent access to

inappropriate material. However, there is a very small risk that inappropriate material might occasionally get through unfiltered. Therefore, our IT support and the SLT regularly review the effectiveness of filtering.

The leadership team and DSLs take shared responsibility for the oversight of filtering and monitoring. This includes an annual review and verification testing to ensure filters are functioning effectively. AI-generated contented is also considered under the filtering and monitoring framework to prevent exposure to harmful material.

The school is committed to maintaining a secure and resilient digital environment. Cybersecurity forms part of our safeguarding provision, including system updates, strong passwords, secure configuration, and incident response procedures. The Headteacher and Governing Body oversee cyber resilience in line with DfE Cyber Security Standards for Schools.

We therefore follow the agreed guidelines below to ensure that children can access the Internet safely.

3. Staff Responsibilities and Safe Practice

Online safety is included in staff induction and regular safeguarding updates. All staff receive annual training on online safety, including new and emerging risks.

All staff must ensure that they:

- Have received adequate training before supervising pupils' use of the Internet or digital devices.
- Supervise children *at all times* when accessing the Internet.
- Educate pupils in safe online behaviours and model responsible use (see Appendix 3).
- Understand and implement guidance on the appropriate use of AI tools, personal devices, and online communication with pupils.
- Give children clear objectives for Internet use (e.g. structure children's access by specifying a site within which they are allowed to browse, use Google Classroom to share links to appropriate sites or by providing lists of suitable websites from which the children should not stray).
- Preview any websites, videos and media they intend to allow children access to, to ensure the media does not contain inappropriate material and is suitable for the age and maturity of their pupils.
- Preview or remove any adverts that are attached to media when streaming videos (YouTube, for example).
- Highlight the need to respect copyright of materials on the Internet and acknowledge the source of materials taken for use in pupils' own work.

- Be aware of the increase in cyberbullying, grooming and radicalisation and immediately report any concerns to the Computing Lead, the Headteacher or Pastoral Lead who will then take appropriate action. Any issue or action raised will be recorded on CPOMS with the E-safety tab to the DSLs and online safety lead.

- Ensure children are aware of the importance of not clicking pop-up links and gaining permission to respond to the pop-up if needed.

Staff should take prompt action if they, or their pupils, encounter inappropriate material on the Internet.

Staff should:

- Ensure children are shielded from unpleasant material (e.g. switch off the monitor and move children away).

- Record the Uniform Resource Locator (URL) or website address, the content of the site and any other relevant information.

- Inform the Headteacher/ Pastoral Lead/Computing Lead of the site details as soon as possible.

The Headteacher/Computing Lead will then:

- Report the inappropriate material and website address to Andy Fielder at South Farm CPA to check files on the system if they believe a child may have been attempting to access unsuitable material.

- The Headteacher and Computing Lead will make occasional checks on files to monitor compliance with the school's policy.

- Discipline children if they make inappropriate use of the Internet. Consequences should be in line with the St Peter and St Paul's Behaviour Policy. These may include suspending a child's access to the Internet and informing parents of serious incidents. The Headteacher should be informed of all incidents where a child has needed sanctioning for irresponsible use of the Internet.

- No discs or external hard drives, brought in from home by the children, should be used on the network as this may introduce a virus to the system.

When using cloud-based learning platforms (e.g. Google Classroom), staff need to be aware of messaging systems within the platform to either disable the feature or teach the children how to use the platform in line with our school rules and values.

Monitoring the use of communication on the platform:

- Messages to children should be checked by a teacher, wherever possible, before being read by children.

- All information posted on Google Classroom by staff and children

should be checked by a teacher before it is sent.

The school will:

- Inform all parents that their children will be provided with supervised Internet access as part of the school's curriculum.

- Inform all parents of the Responsible Use Rules and 'Be Internet Legends' pillars which their children will be expected to use, in order to ensure a safe environment.

- Answer parents' queries and concerns about their child's use of the Internet and our safeguards to protect them from unpleasant material.

- Ensure that there are appropriate filters in place to prevent access to inappropriate content (currently RM filters are used).

- Remind the children about the safe use of the Internet and digital technologies regularly (e.g. during anti-bullying week, Safer Internet Day, online safety assemblies, individual lessons taught at an age-appropriate level, annual signing of age-appropriate ICT Acceptable Use Agreement).

- Use of Virtual Private Networks (VPNs) on school devices or networks is strictly regulated to ensure compliance with safeguarding protocols and monitoring; unauthorised VPN use that bypasses school security measures is prohibited.

For further information regarding Remote Learning and Google Classroom – please see remote learning procedures.

5. Pupil Guidance

Pupils are expected to:

- Agree and follow the ICT Acceptable Use Agreement (Appendices 1 and 2)

- Agree and use the 'Be Internet Legends' pillars (Appendix 3)

- Respect copyright and acknowledge the source of material they have used from the Internet.

- Inform a teacher immediately if they encounter any material that they feel is offensive or they think may cause offence to others.

- Be aware that their files may be reviewed by the teacher at any time.

- Be aware that they will incur sanctions if they make irresponsible use of the Internet.

- Only send polite messages to their teacher as specified and not include personal details (e.g. address, phone number).

6. Parental Involvement

Parents are informed that their children will be provided with supervised Internet access as part of the curriculum. Parental permission will *not* be called for by the school before a child is allowed to gain access to the Internet. Parents will receive guidance on safe online behaviour, including how to support their child at home.

7. Reporting Concerns

Any concerns about online behaviour, harmful content, or misuse must be reported immediately to the DSL, Headteacher, or the Computing Lead. Incidents will be recorded on CPOMS and dealt with in accordance with the Behaviour and Safeguarding policies.

Appendix 1: Responsible use

St Peter and St Paul C of E Primary School

Rules for Responsible Internet Use

- The school has computers with Internet access to help our teaching and learning. These rules will keep you safe and help us be fair to others.
- I understand I must only use the Internet and the computer for school work as directed by the teacher.
- I will ask permission from a member of staff before using the Internet.
- I will only look at or delete my own files.
- I will not use Internet chat at school.
- I understand that I must never give my home address or telephone number, or arrange to meet someone on the internet.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files and may monitor the sites I visit.
- I understand that there are safe and unsafe ways of using the Internet and I will keep myself safe.
- I will take care of school ICT equipment.
- I will hand any electronic devices in to the class teacher during school hours e.g. phones and smart watches.
- I understand that if I deliberately break these rules, there will be sanctions and I may not be allowed to use the Internet or computers.

Name of child ……

Signature of parent/carer …….

Signature of child ……..

As part of ongoing monitoring of access to technology in our community, we would be grateful if you could identify whether, as a family, you are able to access the internet at home.

We have access to the internet at home ☐

We do not have internet access at home ☐

Appendix 2

Pupil Acceptable Use Agreement for EYFS and KS1

	I will keep my password safe and not share it with anyone.
	I will only use a computer when an adult tells me I can.
	I will always send polite and kind messages.
	I will tell an adult if something I see online makes me feel unhappy.
	I will look after the equipment.

Pupil Acceptable Use Agreement for KS2

	I will keep my password safe and not share it with anyone.
	I will only use a computer and the internet when an adult tells me I can.
	I will only look at, edit and delete my own work.
	I understand that I must never give out my personal details online e.g. my name, age, address and school.
	I will tell an adult if something I see online makes me feel unhappy.
	I will take care of the school ICT equipment.
	I know that my teacher will check what I do online. If I break the rules, I understand that I might not be allowed to use digital technology and the internet in school.
	I will hand any electronic devices (e.g. phones and smart watches) in to the class teacher during school hours.

Appendix 3: Google Pillars



Appendix 4 (National Curriculum – Computing)

Key stage 1

Pupils should be taught to:

- understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key stage 2

Pupils should be taught to:

- design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output
- use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
- understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.