St. Peter's Primary School

St. Peter's Anglican Methodist VC
Primary School

Dream, Believe, Achieve

"All things are possible." Mark 9:23

E-Safety Policy

School Address	Bank Road Pilning South Gloucestershire BS35 4JG
School Contact Number	01454 631137

Introduction

At St Peter's we believe that COMPUTING is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

COMPUTING in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up to date technologies in both the suite and classrooms. COMPUTING is a life skill and should not be taught in isolation.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of COMPUTING within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- The use of generative AI (Artificial Intelligence)

All users need to be aware of the range of risks associated with the use of these Internet technologies. At St Peter's Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks'
(Becta Safeguarding Children Online Feb 2009)

This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

Whole school approach

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.
The COMPUTING leaders will ensure they are up to date with current guidance and issues through organisations such as South Gloucestershire and CEOP (Child Exploitation and Online Protection), Integra advice and Child Net.

They then ensure that the Head teacher; Senior team and Governors are updated as necessary.
All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community
- their role in providing e-safety education for pupils.
- promoting the awareness of misinformation, disinformation, and conspiracy theories in accordance with KCSIE (2025 update).
- filtering and monitoring including the use of generative AI (Artificial Intelligence)

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction.

E-safety in the curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

- We provide opportunities within the COMPUTING and PSHE curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the COMPUTING curriculum.

- Pupils are aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the COMPUTING curriculum
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know

The Use of AI (Artificial Intelligence)

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Managing Internet Access

Children will have supervised access to Internet resources

- Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.
- Our internet access is controlled through the **Integra web filtering** service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to a COMPUTING leader, technician or member of SLT.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

Filtering and Monitoring Standards

We provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

- The Designated Safeguarding Lead (DSL) is responsible for ensuring the standards are met.
- Integra is St Peter’s External Service Provider

It is the responsibility of the DSL and the SLT to:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why

- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

The DSL takes lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

The filtering and monitoring provision at St Peter's is monitored annually. Our filtering system blocks harmful and inappropriate content, without unreasonably impacting teaching and learning.
There are effective monitoring strategies in place that meet the safeguarding needs of the school. Further information can be found at https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges.

E-mail

The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school, between schools or international. We recognise that pupils need to understand how to style an email in relation to their age.

- Pupils are introduced to email as part of the Computer Science Scheme of Work.
- The school gives staff their own email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff must inform a member of SLT if they receive an offensive e-mail.
- Staff professional communication via email must only be done through a school email account.

- Response to parents email must be done reasonably within a 24 hour period and within acceptable working week day hours. Staff may respond to email outside of these hours at their own professional discretion.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school web site
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

Social networking and personal publishing

We block/filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Parents will be shared relevant information to age ranges for relevant social media sites to guide them in their children's appropriate use.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Classes have been issued with an iPad to use for school photography, assessment notes, emails, music and educational applications.

Data protection (GDPR)

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

The Act requires schools to:

- Keep personal information safe and secure.
- Protect personal information from misuse.
- Process data securely and confidentially.
- Ensure that all the information they hold about data subjects is accurate.
- Only collect and hold data for its intended purpose.

- Give data subjects control over the use of their personal data.
- Ensure that third parties with whom they share data also process data securely.
- All GDPR requirements are followed in accordance with the school's Data Protection policy (June 2023)

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
Further guidance can be found at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Responding to e-safety incidents/complaints

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Head teacher.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Head teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of COMPUTING, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site. Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour and can include (but not limited to):

- excluding a child from online games, activities or friendship groups
- sending threatening, upsetting or abusive messages
- creating and sharing embarrassing or malicious images or videos
- 'trolling' - sending menacing or upsetting messages on social networks, chat rooms or online games
- voting for or against someone in an abusive poll
- setting up hate sites or groups about a particular child
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum.
They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on
www.kidscape.org and www.wiredsafety.org

Supporting the person being bullied
Support shall be given in line with the behaviour policy…

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the pupil who they have sent messages to.

Investigating Incidents
All bullying incidents should be recorded and investigated in the incident log as any other bullying incident. We will then investigate fully as any other bullying incident (refer to behaviour policy and anti-bullying policy).

Working in Partnership with Parents

Parents/carers are asked to read through and sign acceptable use of COMPUTING agreements on behalf of their child on admission to school (see appendix 1).

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website)
- A partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use.
- Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

This policy will be reviewed by the Inclusion, Achievement, Teaching & Curriculum committee in line with the overall policy timetable which is annually

Policy Agreed

By the Inclusion, Achievement, Teaching & Curriculum Committee on 27 November 2025

Links to other policies
Anti-bullying Policy Behaviuor Policy Computing Policy Dara Protection Policy Safeguarding Policy

Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil

Class

Signed Date

Staff (and Volunteer) Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password 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, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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 the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to 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 is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. 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 of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- 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 School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / 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 school 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.

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 and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name	
Signed	
Date	

Parent / Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside 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. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *pupils* will have good access to ICT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work.

Permission Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son’s / daughter’s activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s e-safety.

Signed Date

Using images of children
Consent form for use by
St Peter’s Anglican/Methodist Primary School

Name of child ____

We sometimes take photographs of the children at our school. We use these images to help us to give people an idea of what life at our school is like for example in the newsletter, on our website or on project display boards in the school. We may also make recordings for monitoring or other education use. Photographs may also be taken at other schools when pupils attend events e.g. enrichment, sports and school cluster activities.

Learning journals and Records of Achievement are used to celebrate children’s progress in the school. Photographs of individuals, groups or classes of children may appear in these records.

From time to time, our school may be visited by the media who will take photographs or film footage of a high profile event. Children may appear in these images, which will sometimes be published in local or national newspapers, or on approved websites or televised news programmes.

To comply with the Data Protection Act 2018, we need your permission before we can photograph or make any recordings of your child. Please answer the questions below, then sign and date the form where shown.

Please return the completed form to the school as soon as possible

Please circle your answer

I give permission for the school to take photos of my child	**Yes / No**
I give permission for my child’s photo to be used within school for display purposes	**Yes / No**
I give permission for my child’s image to be used in Learning Journals/Records of Achievement belonging to other children	**Yes / No**
I give permission for my child’s photo to be used in the school newsletter	**Yes / No**
I give permission for my child’s photo to be used on the school website	**Yes / No**
I give permission for my child’s photo to be used in other printed school materials, for example marketing material	**Yes / No**
I give permission for my child’s photo to be used in the media, i.e.local newspapers	**Yes / No**
I give permission for my child to have a school photograph taken. I understand this printed/digital photograph can be purchased by parents	**Yes / No**
I give permission for the school to take videos of my child	**Yes / No**
I give permission for the school to use videos of my child for promotional purposes such as on the school website	**Yes / No**

I have read and understood the conditions of use on the back of this form.

Parent / Carer signature ……………………………………………. Date ………………………….

Name (in block capitals) ……………………………………………………………

You may alter these permissions at any time, you can let us know by emailing office@stpetersprimary.co.uk, calling the school on 01454 631137 or calling into the school office in person.

Conditions of use

1. This form is valid indefinitely from the date you sign it.

2. We will not re-use any photographs or recordings a year after your child leaves this school. Historic photographs will remain on our school website.

3. We will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications.

4. If we use photographs of individual pupils, we will not use the full name of that child in the accompanying text or photo caption.

5. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.

6. We may include pictures of pupils and teachers that have been drawn by the pupils.

7. We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations".

8. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

Please note that website and social media platforms can be viewed throughout the world and not just in the United Kingdom where UK law applies.