Andy Snipp, BA Hons
Headteacher

St Peter's Church of England Middle School

E-SAFETY Policy

This policy was adopted on 7th June 2019

The policy is to be reviewed in June 2022

Headteacher Andy Snipp

Chair of Local Governing Body Rebecca Scott Saunders

E-Safety

Our e-Safety Policy has been written by the school, building on the RBWM policy framework adapted from the KCC e-safety policy and government guidance. The e-Safety Policy and its implementation will be reviewed annually. The e-Safety Co-ordinator is the Designated Child Protection Office.

When staff, pupils etc leave the school their account or rights to specific school areas are disabled.

Aim of the Policy

- e-Safety concerns, safeguarding Children & Young People in the Digital World.
- e-Safety emphasises, learning to understand the use of new technologies in a positive way.
- e-Safety is less about restriction and more about the risks so we can feel confident on-line.
- e-Safety is concerned with supporting children and young people to develop safer on-line behaviour both in and out of school.

Why is Internet use important ?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

How can Internet use enhance learning ?

- The school Internet access is designed expressly for student use and will include filtering appropriate to the age of students.
- Clear boundaries are set for the appropriate use of the Internet and digital communications and discussed with staff and students.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.
- They are also taught to acknowledge the source of information used and respect copyright when using Internet material in their own work.

How will information systems security be maintained ?

- Virus protection is installed and updated regularly.

- Personal data sent over the Internet or taken off site will be encrypted.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- The security of the school information systems and users is reviewed regularly.

How will e-mail be managed ?

- Students may only use approved email accounts on the school system.
- Students must immediately tell a teacher if they receive offensive email.
- In email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- Staff should only use school email accounts to communicate with pupils as approved by the Leadership Team.

How will published content be managed ?

- Student personal contact information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Can pupil's images or work be published?

- Photographs that include students will be selected carefully so that an individual student's image cannot be misused
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.

How will social networking, social media and personal publishing be managed ?

- The school will control access to social networking sites and educate students in their safe use.
- Students are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Students are advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others. This advice is given in whole school assembly by specialist trainer.
- To support the use of IT being used in all subject areas, staff are trained by a specialist trainer in e-safety.

.

How will filtering be managed?

- The school will work in partnership with the specialist IT company and Internet Service Provider to ensure that systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Co-ordinator or the School Business Manager.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment

- will be carried out before use in school is allowed.
- Students are not allowed mobile phones or tablets in school unless specific permission
- is given by the Headteacher.
- Staff will have use of a school phone where contact with students is required.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

How will Internet access be authorised?

- All staff must read and sign the Acceptable Use Policy before using any school ICT resource.
- Students are asked to agree to the Acceptable Use Policy before they are able to use the school network.

How will risks be assessed?

- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher.

How will Cyberbullying be managed?

Cyberbullying (along with all forms of bullying) will not be tolerated in school.
There will be clear procedures in place to support anyone affected by Cyberbullying.

How will the policy be introduced to pupils?

- All users will be informed in assemblies that network and Internet use will be monitored.
- Issues of e-Safety and how to report abuse will also be covered in lesson time.
- e–Safety is covered by a specialist external trainer annually, covering both safe school and home use.
- e-Safety rules are posted in rooms with Internet access.

How will the policy be discussed with staff?

- Staff are informed that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.
- To protect all staff, the school has implemented an Acceptable Use Policy that all staff sign.

How will parents' support be enlisted?

- Parents' attention is drawn to the School e–Safety Policy in newsletters and on the school website. Parents are also invited to attend a 'Safer Internet Use' evening at school to increase awareness and signpost relevant organisations.

Acceptable Use of ICT Policy for Staff and Volunteers

To ensure that members of staff and Volunteers are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy and Staff Code of Conduct for their information and clarification.

- I understand that is it a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Co-ordinator, the Designated Child Protection Officer or Headteacher.
- I understand that I must not engage with students through social networking. If a student has left the school they are still not to have contact with staff via social networking. This is also the case if a member of staff has left the school.
- I will promote e-Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and Acceptable use policy for ICT:	
Signed	**Date**
Accepted for School	

Student ICT Acceptable Use Policy

I agree to keep my personal information safe.

Be careful what information you put on the internet and who can see it. Use a nickname online and be very careful about what you privacy settings on sites like Facebook. This can help keep you safe.

Don't give out personal information like email addresses, home or school addresses or mobile phone numbers to people you do not know. Do not give information about clubs you are in or where you are at specific times.

*Only post photographs which you would be happy with your parents/carers seeing and make sure they don't show where you or others live. Once a photograph is online, you can **never get it back** or stop it being sent to others.*

Do not share your passwords and log in details as people could access your information without your permission.

I agree to only access sites that are appropriate for my age or download appropriate content and I will tell adults about any sites that I am worried about.

*Some sites include inappropriate content like pornography, violence, racism, sexism and gambling. It is not appropriate to access these sites, and **often against the law**. It is also inappropriate to access sites in lessons that **distract you or others from learning**. You should not attempt to get around any security systems in school, they are there for your protection and safety. If something you need for work is blocked, ask a member of staff to help you.*

I agree to always ask my parent/carer for permission to meet people that I have met online.

Some people on the internet are not who they say they are. Be careful who you chat to and make friends with on Social Networking sites like Facebook. Never agree to meet anyone without telling an adult.

I agree to report my worries I have to an adult.

If an online, message makes you worried or uncomfortable tell an adult, such as a teacher or family member or friend. You can also click on the 'Report abuse' button on many websites, don't reply to upsetting messages or if you feel bullied online. Keep a copy of the message and show it to an adult you trust.

I agree to only send appropriate content via internet.

Never send any video clips, films, pictures or documents that are in any way inappropriate, offensive or illegal.

I agree not to use digital technology to write hurtful comments, bully or make threats.

Always respect others - cyberbullying is not acceptable and does cause distress. This is now an offence, the police can be called and people can be charged with harassment. Treat people as you would like to be treated.

I agree to take care to protect hardware and software.

You will be told the ICT classroom school rules by your teacher and regularly reminded of them, for example, the rules will be displayed in the classroom. Your files and online activities may be monitored by your teachers.

I agree to follow all ICT classroom school rules.

This includes protecting the ICT equipment from spillages by not eating or drinking near computers. You should check any files brought in on memory cards, USB sticks or CDs to ensure they are free of viruses and other malware before use. You should take care of all ICT equipment and report any instances of vandalism to a member of staff.

My teachers, my parent/carers and other adults can provide me with knowledge, guidance and support to help protecting myself from potential danger and harm while using ICT. However, I am responsible for my actions and it is my responsibility to keep myself and others safe online and while using other technologies.

I understand that the school must take appropriate action if I have broken the Student Acceptable use Policy. The school may decide to inform my parents and/or take appropriate action such as; give a sanction/warning, detention, isolation or exclusion. I understand that this may mean restricting my access to the school ICT systems, limiting my use of the internet, restriction / reduction of file space, USB devices or printing or even confiscating my personal equipment to protect me, other users and the network as a whole.

Name: **Signed:** **Date:**

If you want to find out more about using digital technology safely go to: **www.thinkyouknow.co.uk** **Digital safety advice** or **www.ceop.gov.uk** **Report Abuse Button**

e-Safety Audit – Secondary/Middle

This self –audit should be completed by the member of the Leadership Team (LT) responsible for e-safety policy. Staff that would contribute to the audit included: SENCO, School Business Manager and Headteacher.

Has the school an e-safety Policy that complies with RBWM guidance?	Y/N
Date of latest update (at least annual):	
The school e-Safety Policy was agreed by governors on:	
The Policy is available for staff at:	
The Policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Co-ordinator is:	
The e-Safety Co-ordinator is:	
Has e-Safety training been provided for both students and staff?	Y/N
Is there a clear procedure for a response to an incident of concern?	Y/N
Have e-Safety materials from CEOP been obtained?	Y/N
Do all staff sign an Acceptable Use on appointment?	Y/N
Are all students aware of the School's e-Safety rules?	Y/N
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the school e-Safety rules?	Y/N
Are staff, students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by LT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DFE requirements?	Y/N
Has the school-level filtering been designed to reflect educational objectives and approved by LT?	Y/N
Are staff with responsibility for management filtering, network access and monitoring adequately supervised by a member of LT?	Y/N
Have appropriate teaching and/or technical members of staff attended training on the filtering system?	Y/N

Response to an Incident of Concern

Contacts:
Windsor Police :
0845 850 5505

Child Exploitation and Online Protection Centre (CEOP)
www.ceop.police.uk

e-Safety incident occurs

If a child is at immediate risk

Inform the Designated Child Protection Officer and follow school's Child Protection procedures

Consult with Children's Safeguarding Unit (CSU)

Contact Police (999) urgently if there is immediate danger

Illegal Activity or Material found or suspected

Content

e-Safety/CP Officer

Report to Internet Watch Foundation (www.iwf.org.uk) and Police

Activity

Child

e-Safety/CP Officer

e-Safety/CP Officer

Child Protection procedures and/or criminal action

Staff

e-Safety/CP Officer

Staff Allegations procedures and-or criminal action

Unsure

Consult with CSU or e-Safety Officer

Inappropriate Activity or Material

Activity

Child

Possible School Actions:

- Sanctions
- Citizenship
- Restorative Justice
- Anti-bullying
- Parental work
- School support, eg. Counselling, peer mentoring
- Request support/advice from e-Safety officer

Staff

Possible School Actions:

- Staff Training
- Disciplinary action
- School support, eg. Counselling
- Request support/advice from e-Safety Officer

Content

Report to filtering manager and/or School Broadband helpdesk

Local Contact Details:

Schools Designated Child Protection Officer: Andy Snipp

School e-Safety Co-ordinator: Andy Snipp

e-Safety/Child Protection Governor (s): Susan Newell

Safer School Partnership Co-ordinator: PC Graham Slater