St Peter's Bratton Church of England Academy
E-Safety Policy

E-Safety Policy- Document Status			
Date of Policy Creation	February 2023	**Named Responsibility**	Mark Davis
Next Review Due	February 2024	**Named Responsibility**	Zoe Crooke/Lisa Wildgoose

ICT in the 21st Century is seen as 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, at St Peter's we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. E-safety is not just about technology, it is also about people and their actions.

It involves pupils, staff, governors and parents making best use of technology, information, training and this policy in order to create and maintain a safe online and ICT environment for St Peter's School.

E-safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside, is integral to a school's ICT curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and relationships and sex education (RSE) and includes how students should report incidents (e.g. The Child Exploitation and Online Protection (CEOP) button, via a trusted adult, Childline etc). These buttons are displayed on the school website. Teachers receive annual E-Safety training through The Key. They also undertake two additional staff meetings focussed on safer internet information.

In association with the appropriate Acceptable Use Policy Agreement (AUP), this policy forms part of the school's commitment to educate and protect all users when accessing digital technologies, both within and outside school. It should be read in conjunction with other relevant policies, Child Protection/ Safeguarding, Behaviour and Anti-Bullying policies. In England, schools are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. Since 2015 there have been additional duties under the Counter Terrorism and Security Act 2015, known as the 'Prevent duty', which require schools to ensure that children are safe from terrorist and extremist material on the internet, to prevent people from being drawn into terrorism.

Prevent duty requires school monitoring and filtering systems to be fit for purpose. The school has a filtering system in place (referred to in a later section) and its effectiveness is continuously monitored by Mr Adam Harris (Gold support technician) and Mrs A Martin (Vice Principal).

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalization and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviors that increases the likelihood of, or causes, harm, such as 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

Our e-safety Policy has been written by the school, following government guidance (including Keeping Children Safe in Education. It has been agreed by teachers and senior leaders and reviewed by the Local Academy Commitee. E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors and the Computing team, aims to embed safe practices into the culture of the school.

- The school's e-safety coordinators are the 'Computing team'.
- The Designated Safeguarding Lead – Mr M Davis.
- The Deputy Senior Designated Safeguarding Leads are:- Mrs A Martin and Mrs E Oakley.
- The Deputy Designated Safeguarding Leads are :- Mrs N Lewis, Mr R Wilkes, Ms C McCunnin.
- Wrap around care staff DDSLs are:-Miss G Wyatt, Miss L Woodfinden, Miss E Taylor and Mrs D Kelly.
- The Safeguarding Governor is Peter Taylor .
- The e-safety Policy and its implementation shall be reviewed annually, following updates to Keeping Children Safe in Education.

Roles and Responsibilities

Governors

The Safeguarding LAC member meets regularly with the DSL and DDSL and then r who can then reports back to the LAC.

- LAC members ensure that they have read and understood this policy,
- LAC members agree and adhere to the terms on the acceptable use policy
- LAC members ensure online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures

Principal (who is the e-Safety Co-ordinator)

- The Principal is responsible for ensuring the safety (including e-Safety) of members of the school community.
- The Principal is responsible for ensuring that all relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train others colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support ofthose in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Principal should be aware if the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Principal will take day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- The Principal ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- The Principal liaises with school ICT technical staff and the Deputy Principal who is the strategic lead for ICT.
- The Principal/Vice Principal reviews violations on Senso. Teaching staff are also able to view the children's devices via Senso.

Staff

- Staff should read, understand and implement this policy consistently
- Agree to the schools acceptable use policy and ensure that children follow it at all times.
- Ensure that online safety incidents are logged and reported to a DSL
- Deal appropriately with incidents of cyber-bullying
- Respond appropriately to reports and concerns about sexual violence and/or harassment, and

maintain an attitude of 'it could happen here'

Teaching and Learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. It is used to raise the standards of education, support professional work of staff and enhance the schools management. Primarily, it is used to promote pupil achievement.

- The school Internet access will be designed expressly for pupil use including appropriate content filtering
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
- As part of the Computing and PSHE/RSE curriculum, all year groups will have opportunities to focus on different elements of staying safe online. This will include topics such as how to use a search engine, e-mail, apps, digital footprints and cyber bullying. St. Peter's uses Project Evolve materials and follows the Education for a Connected World in addition to marking Safer Internet Day annually.
- Pupils use age appropriate apps and websites within the school setting.
- If a child have loaned a device, due to remote learning needs, their use is monitored as per the AUP (Acceptable use policy)
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture,religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in our school we meet the diverse needs of pupils to ensure inclusion for all and that pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SEN coordinators and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials / content they access online and are guided to validate the accuracy of information.

What we do to keep children with SEND safer online?

It is recognised in our SEND policy that there may be additional risks for children with Special Educational Needs and Disabilities (See policy). St. Peter's Bratton C of E Academy is an inclusive community and therefore the following measures are in place to ensure our pupils can access learning about online safety fairly and in varied ways with the aim to meet all needs of our pupils.

- A robust system for pupils with SEND that identifies needs and provisions for individual pupils
- Staff work with the Special Educational Needs and Disabilities Coordinator (SENDCo), to help provide alternative ways of learning and ensure varied needs can be met through our curriculum offer
- Safer internet day is celebrated annually
- There is regular revision of our E-Safety Policy
- We provide opportunities for staff training on how to keep children safe online, including those with SEND
- Staff consider any additional support/provision for those with SEND required when teaching online safety

The following websites are useful in this area as support for parents :

https://www.thinkuknow.co.uk/professionals/resources/

https://www.internetmatters.org/inclusive-digital-safety/advice-for-parents-and-carers/supporting-children-with-send/

https://www.mencap.org.uk/advice-and-support/bullying-and-discrimination/stay-safe

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable ICT Use Agreement' (Corporate Information Security Policy)
- Parents will be informed that pupils will be provided with Internet access.
- Only school equipment, software and Internet access can be used within the school.

World Wide Web

- The Internet opens up new opportunities and is now an essential part of the everyday world for children: learning, homework and sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time, and content will be recorded by Senso. This violation is then reviewed by the Principal/Deputy Head on Senso.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Telford and Wrekin Council can accept liability for the material accessed, or any consequences of Internet access.

- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible. Within Telford and Wrekin, Senso monitoring software is used throughout the authority and runs behind every software application. The software is designed to protect users and will alert the designated E-Safety co-ordinator of any breaches of the internet use policy. Screenshots are taken by the software at any instance of violation to allow easy tracking of site/words used/user and computer involved.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including skills of knowledge location, retrieval and evaluation. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. All classes will have the age appropriate AUP displayed in their classroom, during the first computing lesson of the term they will be reminded of the policy and with discussion will agree to following it. See Appendix 1.

- We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible for younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching. This includes the use of online videos and games, which are designed to enhance learning.

E-mail and Instant messaging

E-mail and instant messaging are useful and stimulating methods of communication that play an important role in the aspects ofour lives today. We believe it is important that pupils at St. Peter's understand the role of e-mail and instant messaging, and how to use the communication tools appropriately and effectively.

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive an offensive e-mail or instant message, In addition pupils mustalert their teacher if they have received an e-mail/message from someone they don't really know or trust.They are encouraged not to open attachments from these sources.
- Pupils must not reveal personal details of themselves or others in e-mail communication or any other means of communication online (instant messaging, in game chat, video call etc). They should not arrange to meet anyone without agreed parental permission.
- Access in school to external organisations should be written carefully and authorised before sending, in the same way as using outlook.
- The use of TEAMs is to be monitored and the chat function disabled between children. Parent and teacher conversations should be within the child's individual channel during remote learning.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding. Pop ups shall not be clicked on.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff log-on. Staff must always lock their PC if they are going to leave it unattended, even for a short period of time e.g breaktime. They should log out of devices if they have finished using them. Children are reminded of the importance of keeping their password unique to them , not to share their password with others in the class or let others log on as them.

Social Networking

Use of social networking sited and newsgroups in the school is not allowed and will be blocked/filtered Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. The identification of what constitutes as personal information is taught across the school. This will also include not using personal photographs and videos**.** For information and support on social networking and "sexting" please access these sites, which will form the basis and assist with e safety education, support and policy in our school.

http://swgfl.org.uk/
www.thinkuknow.co.uk
www.virtualglobaltaskforce.com
www.parentsprotect.co.uk
www.lucyfaithfull.org.uk
www.stopitnow.org.uk
http://parentinfo.org/

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber-bullying and defamatory comments.

Reporting

All breaches of the e-safety policy need to be recorded in CPOMs. The details of the user, date and incident should be reported.

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.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the Principal on the same day.

Allegations involving staff should be reported to the Principal. If the allegation is one of abuse then it should be handled according to the DFE document titles 'Dealing with allegations of abuse against teachers and other staff.' If necessary, the Local Authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline) .

Mobile Phones

Most mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of image. There are risks of mobile bullying, including peer on peer abuse or inappropriate contact, conduct, commerce or content

- Pupils are not permitted to bring mobile phones or internet enabled smart watches onto the school premises or on school trips andvisits.
- If a child needs to bring a mobile phone to school, for example Y6 walking home alone or an after-school visit, it must be handed into the school office and collected from there at the end of the day.
- Staff should use the school land-line phones or a school mobile to contact parents. Where this is not possible, for example working at home, staff must withhold their number.
- All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the day. Visitor phones are restricted to offices/meeting rooms or are left at the school office.
- Staff may use their mobile phones in the staffroom/one of the school offices. They are not to use their phones when children are in the room (unless they have agreed a specific reason with the Principal).
- Parents and staff cannot use their own mobile phones (apart from the school mobile) on school trips to take pictures of the children.

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'
- Parents and carers are permitted to take photos/videos of their own children in school events. Parents should not upload pictures of their own child/ children onto social networking sites that have been taken at school events. These should be shared through email or private messaging arrangements.
- The Principal or a nominee will inform parent(s)/carer(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Staff should always use a school camera to capture images and should not use their personal devices. The class camera should not be removed from school, unless for a class trip or visit and at the end of the day it should be locked in a secure teacher drawer or cabinet. Photos taken by the school are subject to the Data Protection act.

Published Content, the School Website and School Social Media channel.

The school website and social media channels are valuable sources of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number
- Staff and pupils' personal information will not be published
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate
- Photographs and videos that include pupils will be selected carefully
- Parental permission is sought to display photos of children from St. Peter's on our school website or social media channel (Twitter). Full names are not used and any child who is not allowed to appear on social media will have their image obscured, if they appear in a class or group photo.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Work will only be published with the permission of the pupil.
- Parents should not upload pictures of their own child/ children onto social networking sites that have been taken at school events. These should be shared through email or private messaging arrangements.
- Parents who do not follow the school policy and arrangements explained at an event may be banned from future events.

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with the Local Authority
- E-safety will be discussed with our ICT support and those arrangements incorporated into our agreement with them

Protecting Personal Data

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

The DPO (Data processing Officer) at the St Chad's Academies Trust must review and check all programs which save personal information (eg. Names) before it is used to check that it is a safe place to hold the information. This role is fulfilled by the Compliance Officer.

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. 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

Handling E-Safety Complaints

-
- Complaints are handled by the school complaints procedure, which is detailed on the school website.

Communication of Policy

Pupils:

Users are informed that network and Internet use if monitored and traced to the individual user. E-Safety resources are used within school to teach children safe use of the internet. E-safety rules will be posted in all networked rooms and discussed with the pupils at regular intervals throughout the year. A local community police officer will be invited to talk to the children in KS2 about e-safety at home and at school. E-Safety is taught through a range of child-friendly lessons specifically catered to and differentiated for each Key Stage/Year group to teach them all the elements involved. Integrated into this is an annual safer internet day dedicated to educating the children around the dangers surrounding internet/digital use.
Pupils will be informed of the AUP suitable for their key stage. They will be taught how to follow it and agree to the rules which help them to stay safe online.
A select group of key stage 2 pupils make up a 'Safeguarding Squad' who help to articulate, support and engage the school and wider community in events such as Safer Internet day and Anti-Bullying week. They meet at least once per half term to look at current topics and decide how they will share this with the rest of the school. eg. Assembly on the importance of talking about online experiences.

Staff:

- All staff will be emailed the School e-safety policy and its importance explained.
- Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.
- All staff sign an Acceptable Use Policy at induction.

Parents and carers:

- Parents attention will be drawn to the School e-Safety Policy in newsletters and on the school website. They will also be given an E-safety parental consent form.
- Parents can access a list of internet safety guides and weblinks through the school website.
- Parents are sent up-to-date e-safety newsletters monthly
- Parents are invited to online safety workshops
- Parents can contact DSLs with queries or concerns regarding e-safety

Online security:

The school network and computer system is managed under contract by Telford and Wrekin IDT Managed Services.

As part of this service, internet filtering provision is provided through Smoothwall. This blocks access to the following:
Child sexual abuse content
Terrorism content
Adult content
Offensive language

The DFE recommended testing site provided by SWGfL has been used to verify this.

Classroom monitoring provision is provided by Senso.
More than 99% active web coverage and accuracy Web traffic from 600+ million end users globally. Over 200 languages supported Daily and real-time updates. Senso's filter cloud not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries

Cyber Crime:
The school and Telford and Wrekin IDT Services complies with 10 step EFSA checklist for cybercrime.
This includes:
Home and mobile working
User education and awareness
Incident management
Information risk management regime
Managing user privileges
Removable media controls
Monitoring
Secure configuration
Malware protection
Network security

The school holds a document explaining in detail how online security requirements are met.

Banned items:
Please refer to the school behaviour policy, where this is detailed.

Further Resources

We have found these websites useful for e-Safety advice and information.

Home | CEOP Education (thinkuknow.co.uk)	Set up by the police with lots of information for parents and staff including a place to report abuse

Childnet — Online safety for young people	Non-profit organisation working with others to 'help make the Internet a great and safe place for children'
Keeping children safe online | NSPCC	Advice and support on online safety including cyber bullying and inappropriate and sexual behaviour.
https://www.commonsensemedia.org/	Guidance on app and game ratings and content.
Parent Zone – Parents' area	Digital advice for parents and carers.
https://saferinternet.org.uk/guide-and-resource/what-are-the-issues	Resources and advice for parents, carers and educators.
https://www.taminggaming.com/	Shares research and advice on video games, content warnings and age ratings.