ST PETER'S
CE PRIMARY & NURSERY
SCHOOL WEM

'Underpinned by our Christian values, we create a happy, caring environment. This empowers each and every unique person to dream, believe, achieve and flourish.'

'In the same way, you should be a light for other people.
Live so that they will see the good things you do'

Matthew 5:16 (ICB)

E-SAFETY POLICY
MARCH 2023

Reviewed by: S Kitt, March 2023

Date of next review: March 2024

The Importance of E-Safety

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. Pupils use the Internet widely outside of school and will need to learn how to evaluate Internet information and to take care of their own safety and security. 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 involves pupils, staff, governors and parents making best use of technology, information and training to create and maintain a safe online and ICT environment for St Peter's School. This policy should be read alongside our policies and procedures on child protection and safeguarding.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.
"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."
From: Safeguarding Children in a Digital World. BECTA 2006

Organisation / Provision

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- 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 new Computing and PSHE curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- 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 all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings our SEND co-ordinator and individual teachers to ensure all children have equal access to succeeding in this area.

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

Reporting

All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the general office. 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, via CPOMS, to the Sophie Price, E-Safety Lead and Kirsty Stewart, Character Education Lead in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse, then it should be handled according to the DFE document titled '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, Hector's World dolphin safety button, telling a trusted adult, phoning Childline 0800 1111)

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act, 2018 and Freedom of Information Act, 2000.

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 of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Appendices

1: Detailed information of each area of ICT

2: Further Resources

Appendix 1

Detailed Information on each area of ICT

Internet

Whilst ICT is exciting and beneficial in and out of education, web based resources are not well policed. All users need to be aware of the range of risks associated with the use of these internet technologies and their individual responsibilities relating to the safeguarding of children and themselves, in school and at home.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-safety curriculum. Pupils are aware of the impact of cyber bullying and know how to seek help if they are affected by any form of online bullying.

Managing the Internet

- The school maintains that pupils will have supervised access to Internet resources through the school's fixed and mobile internet technology. All staff will preview any recommended sites before use.
- 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 will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic resources.

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:

- Parents will be informed that pupils will be provided with supervised Internet access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, 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 shall be reported to the teacher who will then report it, by recording the incident in an e-Safety Log, which will be stored in the main office. The e-Safety Log will be reviewed termly by the e-Safety lead.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

Internet Use

- Pupils at St Peters' are too young to use social networking sites, such as Facebook (the legal age limit is 13 years old). However, we recognise children are accessing the sites at home and provide information annually or as necessary to ensure privacy levels are high and children are aware of the risks.
- Annual E safety reminders are taught- specifically in safety week and on Internet Safety Day.

Security

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 logon. Staff must always 'lock' the laptop if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Password security

- Password security is essential for pupils
- Pupils are expected to keep their passwords secret and not to share with others, particularly their friends.

- Staff and pupils are regularly reminded of the need for password security.

Software security

- A security breach, lost stolen equipment, virus notifications, unsolicited emails and all other policy noncompliance must be reported to senior management.
- To minimise risk, pupils should not bring homework to school using portable memory sticks. **Work should be emailed through using year group email addresses.**

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 in to our agreement with them.

E-mail

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the ICT Curriculum.
- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Social Networking

- Social networking Internet sites (such as, Facebook, Instagram, Tiktok, Snapchat, WhatsApp) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites 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. This will also include not using personal photographs and videos.
- 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, family and staff 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.

Mobile Phones

Many mobile phones have access to the Internet and picture and video messaging. These features present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in one of the school offices, out of sight of children.
- Parents cannot use mobile phones on school trips to take pictures of the children.

On trips staff mobiles are used for emergency only.

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. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- The Headteachers or a nominee will inform parent(s)/guardian(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.
Photos taken by the school are subject to the Data Protection Act, 2018.

Published Content and the School Website

The school website is a valuable source 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 Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- 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 only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Appendix 2

Further Resources

We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".