Saint Peter's Catholic Primary School

'Christ in the centre, excellence at the heart'

Mission Statement

To provide a	**C**atholic Education, embracing world faiths,
Nurturing	**H**appy and motivated children
Who want to	**R**each to achieve high expectations
	In partnership with parents
	Supported by a committed staff and Governing Body
Who help children	**T**o feel self-worth and know success

E-SAFETY / ACCEPTABLE USE POLICY

Approving Committee:	LGB
Approved /Adopted Date:	Spring 2022
Signed:	J Connolly (Chair of approving/adopting committee)
Next Review Date:	Spring 2024

The St Peter's Schools e-Safety policy provides details of procedures to be followed relating to e-safety issues and links to further information.

It is revised regularly in line with the Governing Body's policy review.

This policy covers the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It also provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school's e-safety policy operates in conjunction with others including policies for Behaviour, Curriculum, Data Protection, Child Protection, Safeguarding Children, plus the Home-School Agreement and Anti-bullying.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- All internet technologies & electronic communications such as mobile phones, Facebook etc
- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband;
- A school network that complies with the National Education Network standards and specifications.

2.1 Teaching and learning

2.1.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- At times pupils will use an on-line learning platform called Class Dojo to assist with learning at home, be that homework or full lessons (due to full or partial school closure or other factors). This will enable clear communication between pupils, parents and teaching staff and to facilitate continued teaching and learning.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Enhanced teaching and learning.

2.1.3 Internet use will enhance learning

- The school Internet access has been designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are shown how to publish and present information to a wider audience.
- Pupils' use is monitored by adults at all times. There are sanctions for misuse in line with the Governing Body's Behaviour policy.

2.1.4 Pupils will be taught how to evaluate Internet content

- Pupils are taught the importance of cross-checking information before accepting its accuracy.

- Pupils are taught to report misuse/abuse or offensive material through Internet Safety Week and through the computing curriculum scheme of work.

2.2 Managing Internet Access

2.2.1 Information system security

- School ICT systems security is reviewed regularly and monitored by CMAT central IT department & Headteacher who is automatically notified if an attempt is made to access improper material.
- Virus protection is updated regularly.
- Security strategies are discussed with the Senior Management Team.

2.2.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail is treated as suspicious and attachments not opened unless the author is known.
- The school e-mail from pupils to external bodies is presented and controlled by teaching staff.
- The forwarding of chain letters is not permitted.

2.2.3 Published content and the school web site

- Staff or pupil personal contact information is not published. The contact details given online will be the school office.
- The Headteacher & CMAT central IT department take overall editorial responsibility and ensure that content is accurate and appropriate.

2.2.4 Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the school web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names do not refer to the pupil by name. especially when used as content for the school website or social media accounts.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.2.5 Social networking and personal publishing

- The school controls access to social networking sites, and educates pupils in their safe use.
- Newsgroups are blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils are advised to use nicknames and avatars when using social networking sites.
- All school staff are regularly advised of the professional and personal risks associated with the use of social networks, including private facilities.

- All school staff will ensure their social networking sites are not accessible by pupils. Staff are advised of the risks associated with linked content and posts made by others in exposing their accounts to pupils.
- Pupils are helped to develop critical thinking skills to reflect and enable them to keep themselves safe through the computing curriculum.

2.2.6 Managing filtering

- The school works to ensure pupils are protected from unsuitable websites.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the CMAT central IT department and the Headteacher.

2.2.7 Managing videoconferencing & webcam use

Currently not in use.

2.2.8 Managing emerging technologies

- Emerging technologies are examined for educational benefit and risk assessments are carried out before use in school is allowed.
- The senior leadership team are aware that technologies such as mobile phones, smart watches or any smart device with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Pupil's mobile phones should be handed into the office. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Mobile phones should not be used at the school disco.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- Staff are issued with a school ipad to capture photographs of pupils when required.
- The appropriate use of Learning Platforms is discussed as the technology becomes available within the school.
- No photographs are taken on staff's personal phones or cameras.

2.2.9 Protecting personal data

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

2.3 Policy Decisions

2.3.1 Authorising Internet access

- All staff must read and sign the Staff Code of Conduct for ICT (see appendix 1) before using any school ICT resource.
- The school maintains a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents are asked to sign and return a consent form (see appendix 2).
- All children are under adult supervision whilst using computers.
- Student teachers, guests and all personal devices connect to the guest network.

2.3.2 Assessing risks

- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.
- The school cannot accept liability for any material accessed, or any consequences of internet access either from within or outside of school.
- The school audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective. (See appendix 3).
- Should the school need to operate with remote teaching and learning, there are a small amount of laptops that can be borrowed by families who have no suitable hardware. In advance of these laptops being sent out loan agreement (See appendix 4) will be signed, which covers the:-
    - Unacceptable use
    - Personal use
    - Damage/loss
    - Data protection
    - Returning items

2.3.3 Handling e-safety complaints

- Staff must not communicate with pupils (past or present) via social networking sites.
- Staff will ensure their social networking sites are not accessible by pupils.
- 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 must be dealt with in accordance with school's Safeguarding procedures.
- Pupils and parents are informed of the complaints procedure (see schools complaints policy).
- Pupils and parents are informed of consequences for pupils misusing the internet, usually detention after school.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- Complaints of cyberbullying will be dealt with in accordance with the Anti-bullying policy.
- Any e-safety issue will be logged.

2.3.4 Community use of the Internet

- The school liaises with local organisations to establish a common approach to e-safety.

2.4 Communications Policy

2.4.1 Introducing the e-safety policy to pupils

- e-safety rules are posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils are informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, using a computing scheme of work.
- e-Safety training is embedded within the computing scheme of work and the Personal Social and Health Citizenship Education (PSHCE) curriculum.

2.4.2 Staff and the e-Safety policy

- All staff are given access to the School e-Safety Policy and its importance explained.

- Staff are informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use are supervised by senior management and work to clear procedures for reporting issues.
- Staff always use a search engine which is in safe mode when accessing the web with pupils.

2.4.3 Enlisting parents' and carers' support

- Parents' and carers' attentions are drawn to the School e-Safety Policy in Newsletters, policies can be requested from the school website.
- The school has annual e-safety awareness evenings for parents.
- The school asks all new parents to sign the parent /pupil agreement when they register their child with the school.

Appendix 1

Staff Code of Conduct for ICT

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

- I understand that it is 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, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will not store images of children on personal phones, cameras or laptops.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I will not allow children to use the computers without proper adult supervision.
- 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 Designated Child Protection Coordinator or Headteacher.
- I will not communicate with pupils via email, IM and social networking sites.
- I will ensure my social network sites are not accessible by pupils.
- 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 e-mail 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 accept the Staff Code of Conduct for ICT.

Signed: …… Capitals: …… Date: ……

Accepted for school: …… Capitals: ……

Appendix 2

Parental consent form for internet access during lessons

Dear Parent/Guardian

ICT AGREEMENT

St Peter's Catholic Primary School aims to provide children with an understanding of the role computers play in the world around them and the influence that computers can exert. We recognise that ICT will make a substantial contribution to whole school improvement including raising standards of literacy and numeracy.

Through learning the whole range of computing skills laid down in the National Curriculum, and the use of ICT in all curriculum areas pupils will become knowledgeable about the nature of information; comfortable with the new technology; and able to exploit its ever increasing potential.

During this year your child will be accessing the World Wide Web (Internet) with the rest of his/her class. It is our aim to continue to do our best to be vigilant and supervise the material that is available to them when they use the Internet at school. To enable your child to make full use of this valuable resource we ask you to kindly complete the form below and send it back to the school as soon as possible for our records.

Your child's use of school information systems and the Internet maybe monitored and recorded to ensure policy compliance.

Yours sincerely

Mrs L Rinaldi-Oxley
Headteacher

Internet Access

As a parent/guardian, I have read the above policy for access to the Internet and use of the school computer network. I recognise the fact that although the school uses a filtered Internet service, the school staff may have difficulty restricting access to all the controversial materials on the Internet. Therefore I will not hold them responsible for materials that my child may find as a result of using the Internet through school facilities. I take full responsibility for how my child uses the Internet outside of school.

Child's name: ……. Class: …….

Signature of parent/guardian: …… Date:…….

Appendix 3

e-Safety Audit – Primary

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Many staff could contribute to the audit including: SENCO, e-Safety Coordinator and CMAT central IT department.

Has the school an e-Safety Policy?	Y/N
Date of latest update:	
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 responsible member of the Governing Body is:	
The Designated Child Protection Coordinator is:	
Has e-safety training been provided for both pupils and staff?	Y/N
Is there a clear procedure for a response to an incident of concern?	Y/N
Are e-safety units from the computing scheme of work being implemented?	Y/N
Do all staff sign a Code of Conduct for ICT on appointment?	Y/N
Are all pupils 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 pupils?	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, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Is personal data collected, stored and used according to the principles of GDPR?	Y/N
Is Internet access provided by an approved Internet service provider which is deemed safe & secure for pupils to use?	Y/N
Has the school-level filtering been designed to reflect educational objectives and approved by SMT?	Y/N

Device loan agreement for pupils

1. This agreement is between:

1) Saint Peters Catholic Primary School, London Road, Hinckley, Leicestershire, LE10 1HJ and

2) [Name of parent and their address]

This agreement covers the period from the date the device is issued through to the return date of the device to the school and governs the use and care of devices assigned to the parent's child.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the pupil a laptop for the purpose of doing schoolwork from home.

2. This agreement sets the conditions for taking a Saint Peters' laptop home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform the headteacher, and I acknowledge that I am responsible for reasonable costs if requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

- The device should be used solely by the pupil for the purpose of completing school work and not used by anyone else, including other members of the family.
- Pupils should use the equipment in line with the school e-safety/acceptable use policy and should not browse, download or distribute any material deemed to be inappropriate.
- Pupils should not download or install any new software onto the device.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our behaviour/discipline policy, if the pupil engages in any of the above **at any time.**

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected: -

- Make sure my child puts away the equipment in a safe place if it's left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus software as required. Inform the school immediately should the device become infected with malware or a virus.
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact the school office.

6. Return date

I will return the device in its original condition to the school office within 7 days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENT'S SIGNATURE	