St. Peter's Catholic Primary School

# E-Safety Policy

Reviewed by: K Ryan

Date: Sept 2024

Date for next review: Sept 2025

***MISSION STATEMENT***

*St. Peter's Catholic Primary School is at the heart of a Christ centred community where every person's uniqueness is celebrated with joy and truly valued. We foster caring, supportive relationships based on mutual respect and love. We embrace the different communities to which we all belong – home, school and parish, as well as our local, national and global families. When we welcome the child, we welcome the family. We strive for excellence in all we do to be the best that we can be.*

# Introductory Statement

- The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- Children might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails.
- We must ensure that children are equipped with the appropriate technological skills for the future.
- The Internet helps to improve children's reading and research skills.

These far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

This policy is written in accordance with BECTA guidelines, and focuses on each individual technology available within the school and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

The term 'users' refers to pupils. All pupils and staff must complete an Acceptable Users' Policy Agreement (AUP) before accessing the school network and internet.

# Procedures for Use of a Shared School Network

- Staff must access the school network using their personal logons. Pupils must access the school network using their individual logons.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software should not be installed, nor programmes downloaded from the Internet, without prior permission from Mrs Ryan, Mrs Barber or Mrs Russell.
- All members of staff must use OneDrive when saving work. Encrypted pen sticks have the possibility to introduce malware to the school computer system and so must not be used in school.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.

- The school's wireless network is encrypted to prevent outsiders from being able to access it.

## Procedures for Use of the Internet and Email

- All users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment.
- Parental or carer consent is requested in order for children to be allowed to use the Internet or email.
- Children must be supervised at all times when using the Internet and email.
- Procedures for Safe Internet use will be clearly displayed where there are computers with access to the Internet.
- An e-safety assembly will be held annually to remind children about safe internet use.
- An e-safety lesson will be held each half term using the e-safety unit of study from Kapow in Years 1-6.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to Mrs Ryan, Mrs Barber or Mrs Russell and a note of the offending website address (URL) taken so that it can be blocked.
- Use of social media by the children in school is not allowed.
- The use of mobile phones by the children is not allowed anywhere on the school's premises. Older children who bring phones into school as part of their safety in walking home at the end of the day must turn their device off before they enter the school gates and hand their device to their class teacher who will store it safely until home time. Phones must not be turned back on until the child has left the premises.
- Reports of inappropriate, abusive or racist material on any device including children's mobile phones should be reported to the DSL or DDSL immediately. Staff should do their utmost not to view the material or share the information with anyone other than the DSL or DDSL.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.
- Mrs Ryan, Mrs Barber and Mrs Russell receive a weekly update from Network Connect regarding websites that have been blocked by the website filter.
- School receives live alerts from Network Connect if there are any attempts to access blocked content from devices using the school's internet services.
- Email addresses assigned to children will not be in a form which makes them easily identifiable to others. *(Children's email addresses are only used in one computing unit in Year 3 and are only assigned for the duration of that unit with access controlled by the class teacher, computing co-ordinator and IT technician. Emails will only be able to be sent and received within the school).*

- Users must not disclose any information of a personal nature on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- All emails sent from a staff school email account will carry a standard disclaimer disassociating the school and the Local Authority with the views expressed therein.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.
- All email attachments must first be scanned before they can be opened.
- Users must seek permission before downloading any programmes from the Internet.
- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

## Procedures for Use of Cameras, Video Equipment and Webcams

- Permission must be obtained from a child's parent or carer before photographs or video footage can be uploaded to the school website.
- Photographs or video footage will be downloaded as soon as possible and saved into a designated folder. They will then be deleted from the device as soon as possible.
- Adults should not use their own camera, video recorder or camera phone during a trip or visit.

## Procedures to ensure safety of the school's website

- The school has a designated team who is responsible for approving all content and images to be uploaded onto its website prior to it being published.
- The school website should be subject to frequent checks to ensure that no material has been inadvertently posted, which might put children / young people or staff at risk.
- Copyright and intellectual property rights must be respected.
- Permission must be obtained from parents or carers before any images of children can be uploaded onto the school website. Names must not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a

child / young person or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.
- When photographs to be used on the website are saved, names of individuals portrayed therein should not be used as file names.

## Sanctions to be imposed if procedures are not followed

- Letters may be sent home to parents or carers.
- Users may be suspended from using the school's computers, Internet or email, etc. for a given period of time / indefinitely.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.

**Cases of misuse will be considered on an individual basis by Mrs Ryan and Mrs Barber and sanctions will be agreed and imposed as appropriate to each individual case.**

## Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the school and this policy will not remain static. The use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

This policy should be read in conjunction with the:
Computing policy
Child Protection and Safeguarding policy
Behaviour Policy
KCSIE 2024

**K Ryan, headteacher** **Sept 2024**
**Formal review** **Sept 2025**