ST. PATRICK'S CATHOLIC PRIMARY SCHOOL

"Faithfully following in the footsteps of Jesus,
we serve, love and learn together
inspiring each other to excellence."

This policy will be reviewed **every 2 years** by the Governing Body

Online Safety Policy

Nov

Nov

Signed ……………………………..…….….……..…Date……………..…….….……...

Mr T O'Malley
Chair of Governors

Review Date: November 2025

Introduction

As technology advances, we recognise that the internet and the way that society uses the internet can be an immensely powerful and a positive means of communication and collaboration. We know that there are many benefits for our young people in using the internet and other technologies to enhance their understanding of the wider world and how they interact with one another.

The Internet and its effective use is an important part of learning across the curriculum. However, we also recognise that sometimes, internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and challenging situations.

In order to ensure that our pupils are digitally aware and are as safe as possible, we teach specific online safety lessons as part of our Computing curriculum and we have a range of security measures to ensure all pupils are safeguarded within the school setting.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using a range of different technologies and provides safeguards and awareness for users to enable them to control their online experience.

The school's Online Safety Policy should operate in conjunction with other policies including those for Behaviour, Bullying, Data Protection and the school Child Protection Policy.

Online Safety depends on effective practice on a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Have an identified Safeguarding Governor assigned to ensure standards are met
- Sound implementation of the Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering and monitoring systems, recognising that this is everyone's responsibility (KCSIE 2023)

Teaching and learning

Why Internet use is important

- 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 and to ensure all students understand the risks and benefits of internet use.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils and will be taught in line with the National Curriculum at age appropriate levels.
-

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering and monitoring appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Subject Leader for Computing and the DSL for Safeguarding
- Staff should ensure that the use of Internet derived materials by staff and by 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, understanding that Influencers and posts via apps may reflect an opinion, not a fact.
- Children will be made aware at age appropriate levels of cyber bullying and inappropriate online behaviour via specific lessons taught in Online Safety week and Anti-Bullying week.
- Pupils will be made aware of their digital footprint and the idea that digital content will remain available to view, once published.

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly on all devices.
- The school uses broadband with its firewall and filters. The IT service provider and school's broadband provider will work with the senior leadership team and DSL to:
- procure systems
- identify risk
- carry out reviews
- carry out checks
- ensure the filtering provider is a member of Internet Watch Foundation (IWF)

The use of private devices to film or photograph children is strictly forbidden.
All staff will be responsible for filtering and monitoring.

Email

- Pupils may only use approved e-mail accounts on the school system i.e. the Virtual Learning Environment (VLE). Children are not allowed access to personal email accounts or chat rooms whilst in school.
- Pupils must tell a teacher immediately if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Staff will communicate with parents only via school approved email addresses.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published, although class emails for parents will be shared with appropriate year groups and amended each year.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school website will be regularly reviewed and updated.

Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' work can only be published with the permission of the pupil and parents.
- Photographs will only be taken with the school approved camera/iPads.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

- Pupils will receive online safety training that is age appropriate about being safe online.
- Pupils will not be allowed to use mobile phones during the school day.

Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils, e.g. the legal age requirement for Whatsapp is 13+ world wide and 16+ in European countries. Nearly all other social media services require users to be at least 13 years of age to access and use their services. This includes Facebook, Snapchat, TikTok, Twitter, Instagram, Musical.ly and Skype. Whilst there is no age restriction for watching videos on YouTube, users need to be 13 or older to have their own YouTube account. Staff will be made aware through Safeguarding training that harm outside the home can also occur online and in the digital world.

Managing filtering and monitoring

No filtering system can be 100% effective; however, the following procedures are in place to mitigate and minimise harmful content:

- The Governing body has overall strategic responsibility for filtering and monitoring, but daily filtering and monitoring is the responsibility for all staff and any breaches must be reported immediately.
- St. Patricks will appoint a governor to oversee the Filtering and Monitoring and Safeguarding Standards are met
- The DSL and the school will work in partnership with the service provider and broadband provider to ensure filtering and monitoring processes are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the DSL and Computing Subject Leader.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- All staff will receive training on the expectations and responsibilities when filtering and monitoring online content so that they understand their role, follow policies, processes and procedures and act on reports and concerns
- Should filtering and monitoring highlight safeguarding issues, this is to be shared with the DSL/DDSL immediately.

Filtering and monitoring provision, will be reviewed annually or when:

- A safeguarding risk is identified
- There is a change in working practice, like remote access or BYOD
- New technology is introduced
- Additional checks to filtering and monitoring will be informed by the review process thus meeting safeguarding obligations.
- A log of when monitoring and filtering systems are check will be kept and reviewed.
- Blocklists will be reviewed and be modified in line with changes to safeguarding risks

Managing videoconferencing

- Zoom/ TEAMS calls can be used to communicate online (as needed), only when the link has been emailed to the parents preferred email, from the class email address and both parties agree to this communication
- Some video conferencing between parents/ staff may be arranged for specific meetings if needed (e.g SEND meetings)
- Staff may access TEAMS or Zoom for CPD only via links sent to school emails, on school approved devices.
- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- External IP addresses should not be made available to other sites.
- Pupils should ask permission from the supervising teacher (or if at home, parents) before making or answering a videoconference call.

- Videoconferencing should be supervised appropriately for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive, harmful or inappropriate messages is forbidden via text messages or social media Apps
- Staff have access to a school phone where contact with pupils/ parents is required.
- In exceptional circumstances staff may use personal phones (e.g for Parents Evening phone calls) but only if their personal number is blocked and the call has been pre-arranged and agreed.
- Staff and parents have access to a class email, dedicated to that one class to enhance communication. This should be used in a professional and courteous manner, reciprocated by parents, otherwise this could result in the withdrawal of this communication.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Policy Decisions
Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- At EYFS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The headteacher will ensure that the Online Safety Policy is implemented appropriately and that it is monitored and update regularly.
- In the online safety section of Keeping Children Safe In Education 2023 there is guidance on the 4 areas of risk that users may experience when online. All staff will have read this and understand the risks.

Handling Online 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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure via the school website
- Sanctions will be in line with the school Behaviour Policy and may include: – interview/counselling by class teacher / headteacher: – informing parents or carers; – removal of Internet or computer access for a period.

Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Introducing the Online Safety Policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use and accounts on VLE/ Purple Mash can and will be monitored.
- Advice on Online Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet and social media use.

Staff and the Online Safety Policy

- All staff will have access to the School Online Safety Policy and its importance explained.
- The policy will also be available on the school website.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will receive training and information about new developments and updates as needed.

Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the school's Online Safety Policy in newsletters.
- The Online Safety policy will be available on the school website

Appendix 1: Internet use - Possible Teaching and Learning Activities

Activities	Key Online safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Website folder available on school desktop providing a range of suitable websites for access by pupils
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	**Web quests e.g.** Yahooligans CBBC Search Kidsclick Safesearch
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved email accounts e.g. VLE Pupils should never give out personal information. Use 'Thinkuknow' website for children to assess their own knowledge.	Virtual Learning Environment School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website Virtual Learning Environment Espresso Coding PurpleMash
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought.	School website Virtual Learning Environment
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	Virtual Learning Environment
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Not currently in use at St. Patrick's Primary School