

loving laughing learning



Mission Statement

St. Patrick's Catholic Primary School offers distinctive education within a caring Christian community where everyone can feel valued, confident and secure.

We believe that each person is gifted, unique and loved by God.
By working in partnership we create a challenging, stimulating and effective learning environment where Christ is our inspiration.

***Our mission statement is
Loving- Laughing- Learning
We are God's amazing gifts***

E-Safety Policy

Last updated: Summer 2024	
Next Review: Summer 2025	
Headteacher Signature Mary Jenkinson	Vice chair of the LAC Barbara Clements

E-Safety Policy

This policy is to be used in conjunction with the school's ICT and Safe Guarding Policy.

The school will appoint an E-Safety coordinator. In many cases this will be the Designated Safeguarding Lead as the roles overlap.

Our E-Safety Policy has been written by the school following Government and Local Authority guidance. It has been agreed by the senior management team and approved by governors.

The E-Safety Policy will be reviewed every two years. This policy was approved in Summer 2024 and will be reviewed in Summer 2026.

Scope of this policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for all users to enable them to control their online experiences.

The school's E-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection, information sharing and Security. The E-safety policy is in-line with revised Prevent Duty guidelines concerning children's safety from terrorist and extremist material when accessing the internet.

Why Internet and digital communications are important

E-Safety depends on effective practice at a number of levels:

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.
- 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 curriculum and a necessary tool for staff and pupils. The school Internet access is provided by EMBC for Learning and includes filtering, 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 within the E-safety elements of ICT provision. This will be in line with age appropriate content as set out in the National Curriculum
- Pupils will be educated in the effective use of the Internet.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering 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 on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent statement in the pupil information form which refers to the home school agreement; detailing pupil access in the E-safety policy.

Internet use

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Pupils will be taught how to evaluate Internet content

- The school will seek to 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.
- Pupils will be taught how to report unpleasant Internet content through the E-safety provision.
- Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

E-mail

- Pupils and staff 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.
- Access in school to external personal e-mail accounts may be blocked.
- Whole class or group e-mail addresses should be used in school
- E-mail sent to external organisations 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.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- In line with our code of conduct, it is not acceptable for any staff member to be friends on social media with any parent or child (past or present under the age of 18)

- Staff and pupils are not permitted to put things on social media that would bring the school into disrepute
- Parents are not permitted to share any images of school masses, assemblies or any other group activities of other people's children

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video call

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.
- In the event of school closure, teams will be used to communicate as a staff via the individual school emails

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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school mobile phone where contact with pupils is required.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- In addition to the school website: staff, parents and children have access to our internal communication system Class Dojo.
- Class Dojo affords parents and children to send their teachers messages without the need to have individual teacher emails
- The published content is a celebration of children's work and a way of communicating with parents what is going on in school on a daily basis
- This is a closed system and all parents have access to the school story but parents have year group access to the site only
- The school does have a Twitter and Facebook account and minimal content is published on there but any content shared has permission in place

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.

- LAC children will not appear on any public website in line with safeguarding
- Work can only be published with the permission of the pupil and parents.

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.

Protecting Personal Data

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

Assessing Risks

- 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. Neither the school nor Nottinghamshire City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should 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 head-teacher.
- Complaints of a child protection nature must 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 Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Web site. Certain details will be also shared via the home school

agreement and data sharing forms issued to parents at the start of each academic year

E-Safety Audit – Primary Schools

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an E-Safety Policy that complies with CYPD guidance?	Y
The Policy was agreed by governors on: 25th April 2020	
The Policy is available for staff at: School Office	
And for parents at: School office and website	
The designated Child Protection Teacher/Officer is: Miss Jenkinson	
The E-Safety Coordinator is: Miss Jenkinson	
Has E-safety training been provided for both pupils and staff?	Y
Is the Think U Know training being considered?	Y
Do all staff sign an ICT, e safety, data sharing and Code of Conduct policies on appointment?	Y
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y
Have school E-Safety Rules been set for pupils?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access. Furthermore, terrorist and extremist material is blocked.	Y
Has the school filtering policy been approved by SMT?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

Appendices

Referral Process – Appendix A

E-Safety pupil acceptable use agreement Rules– Appendix B

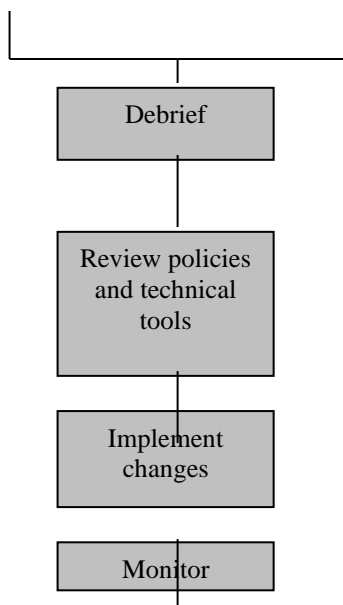
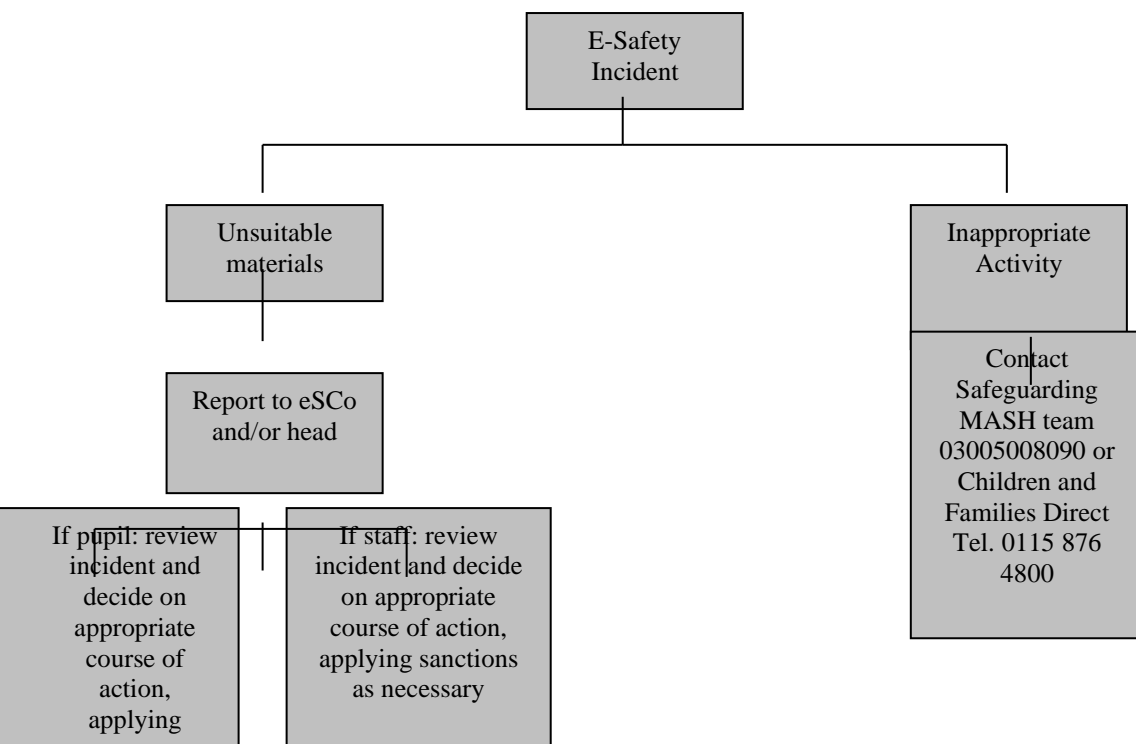
E-Safety parent/carer acceptable use agreement – Appendix C

Staff information Code of Conduct – Appendix D

Em Cloud Web Filtering for schools policies – Appendix E

Appendix A


Flowchart for responding to e-safety incidents in school



Appendix B


Key Stage 1 E-Safety pupils acceptable use agreement

Think then Click
These rules help us to stay safe on the Internet



We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.





We can search the Internet with an adult.

We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.



Key Stage 2

Think then Click

E-Safety acceptable use agreement - rules for Key Stage 2

- *We ask permission before using the Internet.*
- *We only use websites that an adult has chosen.*
- *We tell an adult if we see anything we are uncomfortable with and we will learn about using the CEOP report button.*
- *We immediately close any webpage we not sure about.*
- *We will learn how to use the ‘**thinkyouknow**’ website to keep ourselves safe.*
- *We send e-mails that are polite and friendly.*
- *We never give out personal information or passwords.*
- *We never arrange to meet anyone we don’t know. We are aware of stranger danger and only e-mail people an adult has approved.*
- *We do not open e-mails sent by anyone we don’t know.*
- *We do not use Internet chat rooms or share personal information about ourselves or others without permission.*
- *We know the school can look at our use of ICT and what we see online and we never access other people’s files.*
- *We respect our computer equipment and the work of others and we don’t upload or download images, music or videos without permission.*
- *We do not use mobile phones in school or USB devices without permission.*
- *We do not fill out any online forms without adult permission*
- *We will learn about copyright laws and make sure we acknowledge resources we use.*
- *We understand these rules help us both in school and outside school.*

E-Safety Rules

These E-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user’s authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.

- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

E-safety

Parent/Carer Acceptable Use Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to read these rules and sign the pupil information form which states that they understand and accept the contents of the home-school agreement, including E-Safety Rules.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names. I will not post pictures taken of other children in school on social networking sites.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.

I understand that occasionally inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise according to the policy.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

I understand that my son's/daughter's activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the e-safety rules.

I understand that everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate or malicious comments about the school or any member of the school community.

I understand that Social media websites are occasionally used to fuel campaigns and complaints against schools, Headteacher's, school staff, and in some cases other parents/pupils. I understand that the Governors of St. Patrick's Catholic Primary school, consider the use of social media websites being used in this way as unacceptable and not in the best interests of the children or the whole school community. Therefore any concerns I have will be shared through the appropriate channels following the schools complaints procedures. I also understand that posting libellous or defamatory comments on Facebook or other social network sites, may be reported to the appropriate 'report abuse' section of the network site.

NB: Please note in serious cases school will also consider legal options to deal with any such misuse of social networking and other sites.

Staff Information Code of Conduct

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

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure 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 school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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 agree with the Information Systems Code of Conduct.

Signed: Print

Date:

Accepted for school: Print:

.....

emCloud Web Filtering for Schools – Policies

Category	Primary	Secondary	Staff Elevated
Abortion	Block	Block	Allow
Adult/Mature Content	Force Deny	Force Deny	Force Deny
Alcohol	Block	Block	Allow
Alternative Spirituality/Belief	Allow	Allow	Allow
Art/Culture	Allow	Allow	Allow
Auctions	Block	Block	Allow

Audio/Video Clips	Block	Block	Allow
Brokerage/Trading	Allow	Allow	Allow
Business/Economy	Allow	Allow	Allow
Charitable Organizations	Allow	Allow	Allow
Chat (IM)/SMS	Block	Block	Allow
Child Pornography	Force Deny	Force Deny	Force Deny
Computer/Information Security	Allow	Allow	Allow
Content Servers	Allow	Allow	Allow
Controlled Substances	Force Deny	Force Deny	Force Deny
Dynamic DNS Host	Allow	Allow	Allow
E-Card/Invitations	Allow	Allow	Allow
Education	Allow	Allow	Allow
Email	Allow	Allow	Allow
Entertainment	Allow	Allow	Allow
Extreme File Storage/Sharing	Force Deny Allow	Force Deny Allow	Force Deny Allow
Financial Services	Allow	Allow	Allow
For Kids	Allow	Allow	Allow
Gambling	Force Deny	Force Deny	Force Deny
Games	Allow	Allow	Allow
Government/Legal	Allow	Allow	Allow
Hacking	Force Deny	Force Deny	Force Deny
Health	Allow	Allow	Allow
Humor/Jokes	Block	Block	Allow
Informational	Allow	Allow	Allow
Internet Connected Devices	Allow	Allow	Allow
Internet Telephony	Allow	Allow	Allow
Intimate Apparel/Swimsuit	Block	Block	Block
Job Search/Careers	Allow	Allow	Allow

Malicious Outbound Data/Botnets	Force Deny	Force Deny	Force Deny
Malicious Sources/Mal nets	Force Deny	Force Deny	Force Deny
Marijuana Media Sharing	Force Deny Allow	Force Deny Allow	Force Deny Allow
Military	Allow	Allow	Allow
Mixed	Block	Block	Allow
Content/Pote ntially Adult			
News/Media	Allow	Allow	Allow
Non- Viewable/Infr astructure	Allow	Allow	Allow
Nudity	Block	Block	Block
Office/Busine ss	Allow	Allow	Allow
Applications			
Online	Block	Block	Allow
Meetings			
Peer-to-Peer (P2P)	Force Deny	Force Deny	Force Deny
Personal Sites	Block	Allow	Allow
Personals/Da ting	Force Deny	Force Deny	Force Deny