St Patrick's Catholic Primary School
E Safety Policy

Electronic technologies are an essential part of 21st century life. This E-Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. This policy will be displayed on the school website and should operate in conjunction with other school policies including;

- ✓ Safeguarding Policy
- ✓ Positive Behaviour Management Policy
- ✓ Social Media Policy (school accounts)
- ✓ Computing and ICT Policy
- ✓ Staff Code of Conduct

The E-Safety Policy will be reviewed annually by the coordinator and agreed by SLT using relevant guidance and has been formulated using guidance from LCC Acceptable Use Code of Practice.

Teaching and Learning

1.1 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience. **See appendix 1 – Appropriate Internet Use**

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages across each subject. The Computing curriculum includes an E-safety topic for each year group, which needs to be continually reinforced.

We continually strive to ensure:

- ✓ The school Internet access will be designed expressly for pupil use and will include 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.
- ✓ That the use of Internet derived materials by staff and pupils complies with copyright law.
- ✓ Pupils understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- ✓ Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- ✓ Pupils are 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 deal with inappropriate information online or what to do when they feel threatened or uncomfortable.
- ✓ Pupils will be taught not to reveal personal details of themselves or others in e-mail or online communication, or arrange to meet anyone without specific permission.

1.2 Parents and Carers

Many parents and carers have only a limited understanding of E-safety risks and issues, yet play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimated how often children and young people come across potentially harmful and inappropriate material on the internet and through gaming and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through;

- ✓ Specific E-safety page on the school website
- ✓ Newsletters and letters
- ✓ Published Magazines (eg; Vodafone magazine)
- ✓ Events and campaigns (Eg; Safer Internet Day)
- ✓ Parents training and courses

1.3 Radicalisation and Extremism

Pupils will be taught, through the curriculum, about the dangers of social media and the messages that they may find across the internet. We aim to help them recognise when they and others are at risk and equip them with the skills, strategies and language they need to take appropriate action. Staff will receive the relevant WRAP training to help identify when children may be at risk. Any concerns will be directed to the Safeguard Lead and appropriate action will be taken.

2 Managing Internet Access

2.1 Information System Security

- ✓ School ICT systems capacity and security will be reviewed regularly.
- ✓ Virus protection will be updated regularly.
- ✓ Security strategies will be discussed with LGfL and other providers.

2.2 School Website (www.stpatricksliverpool.co.uk)

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 will take overall editorial responsibility and ensure that content is accurate and appropriate.
Pupils' full names will not be used anywhere on the website, particularly in association with photographs, which will be selected carefully. Written permission from parents or carers will be obtained for photographs of pupils to be published on the school website.

2.3 Social Networking and Personal Publishing

The school will block/filter access to social networking sites (excluding Twitter – *see Social Media Policy)*. Pupils will be advised never to give out personal details of any kind, which may identify them or their location. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Any issues on Social Media, which impacts on school life, will be dealt with in by a member of Senior Leadership Team (*See Positive Behaviour Policy).* The use of such systems by teaching staff should be compatible only with their professional role **(User Code of Conduct for ICT – Appendix 2)**.

2.4 Managing Filtering

The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. Some sites (such as Twitter and You Tube) will be unlocked for educational purposes but must be used appropriately and monitored by staff members **(Appropriate Internet use – Appendix 1)**. In these circumstances, it will be highlighted to children that not everything will be appropriate or consistent with the ethos of our school. If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator or Safe Guard Lead where appropriate. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.5 Managing Videoconferencing

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 **(Appropriate Internet use – Appendix 1)**.

2.6 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 or inappropriate text messages is forbidden. Staff must use a school phone where contact with pupils is required.

2.7 Protecting Personal Data

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

3) <u>Policy Decisions</u>

3.1 Authorising Internet Access

All staff must read and sign the 'User Code of Conduct for ICT **(See Appendix 2)** before using any school ICT resource. At key stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Children will be asked to read and sign An Acceptable Use Agreement – this agreement will be discussed in detail to ensure children's understanding **(See appendix 3, 4 and 6)**.

3.2 Assessing Risks

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. Neither the school nor LGfL can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision on an ongoing basis to establish if the e-safety policy is adequate and that its implementation is effective. However, children will also be taught about e-safety risks, how to minimise these and dealing with them if they arise.

3.3 Handling E-Safety Complaints

Pupil Internet misuse will be dealt with by a senior member of staff. An incident form must be completed and handed to the Headteacher **(see appendix 5 – E safety Incident Log)** and will be dealt with in accordance with *the Positive Behaviour Policy).* Staff will be aware of expectations placed upon them through the Code of Conduct and 'Users Code of Conduct for ICT **(see appendix 2).** 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 safeguarding procedures.

4) Unsuitable/Inappropriate Activities

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Co-ordinator: H.Jones

Date of Policy: September 2020

Review Date: September 2021

Appendix 1: Appropriate Internet use - Possible teaching and learning activities

Activities	**Key e-safety issues**
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
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.
Exchanging information with other pupils and asking questions of experts via blogging.	Pupils should never give out personal information. Consider using systems that provide online moderation. Ensure children are aware of expected behaviours, language and attitude.
Publishing pupils' work on school and other websites.	Pupils' full names and other personal information should be omitted (use of first name is acceptable).
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. File names should not refer to the pupil by name.
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.

Appendix 2: User Code of Conduct for ICT

Toxteth Learning Network
User Code of Conduct for ICT

To ensure that all members of staff and Governors 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. All 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 understand that school information systems may not be used for private purposes without specific permission from the head teacher.
- 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 e-Safety Coordinator, the Designated Child Protection Coordinator or Head teacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- 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.
- I will abide by the terms laid out in the Staff Code of Conduct

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 User Code of Conduct for ICT.

Signed: …… Print: …… Date: ……

Appendix 3 :Pupil Acceptable Use Policy Agreement – Foundation Stage and Key Stage 1

This is how we stay safe when we use computers;

- ✓ I will ask a teacher or suitable adult if I want to use the computers
- ✓ I will only use activities that a teacher or suitable adult has told or allowed me to use
- ✓ I will take care of the computer and other equipment
- ✓ I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- ✓ I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- ✓ I know that if I break the rules I might not be allowed to use a computer.

Child's name - …….

Signed - …….

Date - ……

Appendix 4 - Pupil Acceptable Use Policy Agreement – Key Stage 2

Internet use within school

I understand that I must use the school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. To do this;

- ✓ I understand that the school will monitor my use of the systems, devices and digital communications.
- ✓ I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- ✓ I will not download any software without permission.
- ✓ I will respect others' work and property and will not access, copy or remove any other users' files or work.
- ✓ I will immediately report any damages or faults involving equipment or software, however this may have happened,
- ✓ I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- ✓ When I use the internet for research, I will take care to ensure the information is accurate.

Signed - ……..

Pupil Name - ……..

Date - ……

Internet use outside school

I will ensure I use appropriate language and behaviours while using the internet
I will immediately report anything that makes me feel uncomfortable to an appropriate adult.
I will not share any personal information online.
I will ensure I keep my passwords private and not share them with friends.
I understand that there may be consequences in school if I do anything online that impacts the school.

Signed - ……..

Pupil Name - ……..

Date - ……

Appendix 5: E safety Incident log

E-Safety Incident Log

Please staple any printed evidence to support the incident

Date happened:

Time:

Name of Perpetrator (s):

Name of Victim(s);

Name and date of person reporting incident: *If not reported, how was the incident identified? Include names of all adults to report (Eg; child, parent and staff member).*

Where / how did the incident occur? *(BBM, texting, video call, website, blogging – please give specific site)*

Description of incident: *Please include type in incident (bullying, security risk, hacking, racism, sexual, illegal activities)*

Action taken; *Please include staff members involved in action, any referrals / safeguarding concerns, parental involvement, disciplinary action*

Further action or outcomes: *Please include continuous monitoring, CP file opened / added to, changes to e-safety policy or procedures required*

Appendix 6: Smart campaign