Online Safety Policy

Article 17
You have the right to information that is important to your wellbeing…Adults should make sure that the information you are getting is not harmful, and help you find and understand the information you need.

Rationale

Board of Governors have a duty to safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries (Northern Ireland) order 2003). It is also the duty of the Board of Governors to determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries (Northern Ireland) Order 2003).

In the exercise of those duties, Boards of Governors must ensure that the school has a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. Our approach to online safety is also reflected in our Safeguarding and Child Protection Policy, Promoting Positive Behaviour Policy and Anti-Bullying Policy.

Context

The internet and other digital technologies are a very powerful resource which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business, and social interaction. Our school provides pupils with opportunities to use excellent online resources, along with developing the skills necessary to access, analyse and evaluate them.

However, online safety, in schools and elsewhere, remains a paramount concern. We recognise the crucial role we can play in

- raising awareness of the risks,
- highlighting the impact of behaviour when engaging with online technologies and
- educating children about how to act appropriately and stay safe.

We want pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online. However, in doing so, they need to know how to protect themselves.

We aim to ensure that pupils and adults are kept safe online whilst in school and on school-organised activities. We take seriously our responsibility to ensure the risk of pupils accessing harmful and inappropriate digital content is minimised. We teach all pupils how to act responsibly and keep themselves safe in the digital world and as a result pupils' develop a clear understanding of online safety issues.

In January 2014, the Safeguarding Board for Northern Ireland published its Report '*An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland*'. The report highlights the requirement to take appropriate preventative action to protect children and minimise the associated risks around online safety. These risks have been defined under four categories:

- **Content risks**: The child is exposed to harmful materials.
- **Contact risks:** The child participates in adult-initiated online activity and/or is at risk of grooming.
- **Conduct risks**: The child is a perpetrator or subject to bullying behaviour in peer-to-peer exchange and/or is at risk of bullying, entrapment and/or blackmail.

- **Commercial risks**: The child is exposed to inappropriate commercial advertising, marketing schemes or hidden costs/fraud.

Policy Aims

- To ensure that governors and all staff are aware of their roles and responsibilities in helping children understand how to stay safe online.
- To ensure that all staff are aware of the potential risks posed to children and adults by unsafe online behaviour and to be aware of strategies for staying safe online.
- To ensure that staff and pupils understand procedures for reporting and dealing with issues and concerns around online safety.

Policy Objectives

- All teaching and non-teaching staff can recognise and are aware of online safety risks.
- School staff receive appropriate online safety training and regular online safety information.
- Online safety messages are integrated across the curriculum for pupils in all year groups in age-appropriate ways and actively promoted, including information on how to stay safe; how to protect themselves online; and how to take responsibility for their own and others' safety.
- Online safety messages are distributed amongst pupils, staff, parents/carers and the wider community.
- The ICT Coordinator and the Designated Teacher for Child Protection develop their expertise around online safety.
- Regular and relevant online safety resources and messages are offered and shared with parents via workshops, leaflets and booklets sent home, the school website and social media where appropriate.

Roles and Responsibilities

Online Safety is an important aspect of strategic leadership within the school. The Board of Governors and Principal, aided by the Senior Leadership Team, the Safeguarding Team and the ICT Coordinator, have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current online safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), CyberSafe Ireland and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of online safety throughout the school. However, safeguarding and promoting pupils' welfare around digital technology is the responsibility of everyone who comes into contact with them in the school or on school-organised activities**.**

C2K

Classroom 2000 (C2K) is the project responsible for the provision of an information communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

Features of the safety services from C2K include:

- Providing all users with a unique user name and passwords
- Tracking and recording all online activity using the unique user names and passwords
- Scanning all C2K email and attachments for inappropriate content and viruses.
- Filters access to web sites.
- Providing appropriate curriculum software.

Additional internet provision is provided by Classnet which also has effective firewalls, filtering and software monitoring mechanisms in place.

Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, theft, libel, fraud, discrimination and obscenity. We have a Code of Practice (Appendix 1) for pupils and a Code of Practice (Appendix 2) for staff containing Online Safety Rules which makes explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile internet; school PCs, laptops, iPads and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought onto the school premises (such as mobile phones etc) are subject to the same requirements as technology provided by the school.

The ICT Co-ordinator and the Principal/ Senior Leadership Team will monitor the effectiveness of the code of practice, particularly in light of the additions to the school's technology upgrades.

Code of Safe Practice for Pupils

A parental/guardian consent letter (Appendix 3) accompanied by the Code of Practice will be sent out annually to parents/guardians and this consent must be obtained before pupils access the internet.

In addition, the following key measures have been adopted by St Therese of Lisieux Primary School to ensure our pupils do not access any inappropriate material:

- The school's Online Safety Code of Practice for Use of the Internet and other digital technologies is made explicit to all pupils and guidelines are displayed prominently throughout the school;
- Our Code of Practice is reviewed annually and signed by parents/pupils;
- Pupils using the Internet will work in highly visible areas (ICT suite/ Classroom/ Library);
- All online activity is for appropriate educational purposes and is supervised;
- Pupils will mostly use sites pre-selected by the teacher and appropriate to their age group.
- Pupils in all Key Stages are educated in the safe and effective use of the Internet.

- Pupils are taught and regularly reminded to report anything that concerns/worries them to a teacher/parent as soon as possible.
- Pupils are taught that internet users can be blocked and reported to the online provider if behaviour is inappropriate.
- If pupils bring a phone to school, it must be switched off and left at the office.

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.

The use of mobile phones by pupils is not permitted on the school premises during the school hours. During school hours, pupils are not permitted to play non-educational computer games or access social media.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Promoting Positive Behaviour Policy and Anti-Bullying Policy. Minor incidents will be dealt with by teachers and may result in a temporary ban on internet use. Incidents involving safeguarding/child protection issues will be forwarded to the Designated Teacher for Child Protection and appropriate measures will be taken in line with our Safeguarding Policy.

Code of Practice for Staff

The following Code of Safe Practice has been agreed with staff:

- Pupils accessing the Internet should be supervised by an adult at all times.
- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These will be displayed in the classrooms and discussed with pupils.
- All children using the internet must have written permission from their parents.
- In the interest of systems security, staff passwords must not be shared.
- Teachers are aware that the C2K system tracks all internet use and records all websites visited. The system also logs emails and messages sent and received by individual users.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils should be taken with a school camera/iPad. Only pupils whose parents have given consent can have their photos taken. Images should be stored in a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported as soon as possible to the Principal/ICT Co-ordinator. The coordinator will contact C2k to report concerns. The ICT coordinator records any breaches/potential breaches in an Online Safety Risk Register and subsequent actions.
- Any Safeguarding or Child Protection concerns must be reported to the Designated Teacher for Child Protection (DT) or the Deputy Designated Teacher for Child Protection (DDT) immediately. The DT/DDT will liaise with the Principal and follow the Safeguarding and Child Protection Policy.
- Once off incidences of unkindness online will be dealt with in the same way as in real life, through discussion of our Golden Rules and our Positive Behaviour Expectations. Parents will

be informed if the issues occurred outside of school. Teachers will record minor issues in their class Pastoral Log and monitor the situation.

- If a teacher becomes aware of online bullying or alleged bullying behaviour they will follow the Anti Bullying Policy and record any actions and their outcomes in the appropriate form. Parents of the children concerned will be contacted as soon as possible. Staff will discuss the issue with the Key Stage Coordinator, VP, SENCO and/or Principal as appropriate and will monitor the situation.

Internet Safety Awareness

In St Therese of Lisieux, we believe that alongside having a written Online Safety Policy and Code of Practice, it is essential to educate all users in safe and effective use of the internet and other forms of digital communication. This education is as important for staff and parents as it is for pupils.

Internet Safety Awareness for Pupils

Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, pupils are made aware of and discuss Online Safety through progressive, structured and age appropriate lessons and assemblies. They are taught how to stay safe, how to protect themselves online, how to take responsibility for their own and others' safety, as well as how to block and report inappropriate content.
There are various pupil resources available such as:

FOUNDATION / KEY STAGE 1

- https://www.everyschool.co.uk/i.c.t.-key-stage-1-internet-safety.html
- http://www.123ict.co.uk/meet-smartie-the-penguin-eyfs-e-safety-resources/
- http://kidsmart.org.uk/teachers/ks1/
- 7https://www.thinkuknow.co.uk/5_7/

KEY STAGE 2

- https://gridclub.com/
- https://www.lancsngfl.ac.uk/curriculum/pshe/download/file/signposts_safety_ks1and2.pdf
- http://www.kidsmart.org.uk/
- http://www.childnet.com/resources/kia
- https://www.thinkuknow.co.uk/
- http://www.childnet.com/sorted/

A wealth of resources is also available in a dedicated Fronter Room. A range of engaging picture books are available from the ICT coordinator that highlight online dangers in an age appropriate way for the Foundation Stage and KS1.

Internet Safety Awareness for Staff

The ICT Co-ordinator stays informed and updated on issues relating to Online Safety. All teaching staff and classroom assistants receive regular updates on Online Safety for both the children and the staff themselves.

Internet Safety Awareness for Parents

The Code of Practice is sent home at the start of each school year for parental signature. Additional advice for parents also accompanies this letter. Parents are invited to an Online Safety presentation during Internet Safety Week each year and relevant publications and internet links are forwarded periodically to parents. Community events and information regarding online safety concerns are communicated to parents through the school newsletter and twitter account.

Community Use of School ICT Resources

As an important stakeholder in the Holy Family parish, the school's ICT resources may at times be used as part of the services we provide through our school community use. For this to be enabled, users must be issued with usernames and passwords from C2K. They must also agree to and sign a copy of the school's Acceptable Usage of the Internet Policy. They must only select and use pre-determined and appropriate websites under the guidance of the tutor who is providing the class.

Health and Safety

In St Therese of Lisieux Primary School we have attempted, in so far as possible to ensure a safe working environment for pupils and teachers using ICT resources, both in the classroom and the ICT suite, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used. Guidance is also issued to pupils in relation to the safe use of computers, interactive whiteboards and projectors. With the increased provision of handheld devices, namely iPads, children have also been informed of the need to handle these with care and to report any problems immediately to the teacher or classroom assistant. Children are made aware in the guidance given of the need to sit with good posture, with all chair legs on the ground. They are reminded to adjust the screen to suit their optimum viewing level. Children are reminded not to look directly into the beam of a projector etc. We are also mindful of the impact that ICT can have on certain medical conditions e.g. photosensitive epilepsy. Teachers record all medical conditions that parents make them aware of in their class files and act accordingly upon these.

Use of Mobile Phones/Personal Mobile Technology

Most mobile phones have internet connectivity. Children are not permitted to use mobile phones at any stage throughout the day on school premises. Any child who brings a mobile phone into school must leave it into reception at the start of the school day and collect it at the end of the day. Children are strongly discouraged from bringing their personal mobile technology to school, including hand held gaming devices, because of safeguarding concerns and also due to the high cost of these devices. Teachers will be vigilant especially during Golden Time and ensure that if any devices are brought to school that they are put away securely until they can be handed to parents.

Staff are able to connect their personal mobile phones to the C2K Managed Network through the provision of a usernames and password from the ICT Co-ordinator. As with all C2K provisions, any access to the network will be monitored by the terms of the Acceptable Use of the Internet Policy. All access and communications are monitored and recorded.

Wireless Networks

The Health Protection Agency (HPA) has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available on the Health Protection Agency website.

School Web Site

The school web site is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the website reflects the schools' ethos and that information is accurate and well-presented and that personal security is not compromised. As the school's website can be accessed by anyone on the Internet, the school has to be careful to safeguard the interests of its pupils and staff. The following rules will apply:

- The point of contact on the website is the school address and telephone number and the school and principal's email addresses. Staff or pupils' information will not be published.
- Website photographs that include pupils will be selected carefully. Written permission from parents or guardians will be obtained prior to this through the photographic permission letter at the start of the first academic term.
- Pupils' names will not be used anywhere on the website, particularly in association with photographs.
- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce them has been obtained.

Social Software

This is a generic term for community networks, chatrooms, instant messenger systems, online journals, social media networks and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users. Such software allows users to exchange resources, ideas, pictures and video.

The majority of activity in these online sites usually cause no concern. C2K and Classnet have filtered out these social networking sites so children cannot access them in school. Concerns in relation to inappropriate activities on social media come from use outside the school environment.

Staff will remind parents and children that all social media platforms have a minimum age requirement for usage and should bear this in mind when granting permission to use such a facility. The most commonly used, have a recommended 13 years lower age limit, which means that primary school children should not use them.

However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Online Safety sessions for pupils. As part of our annual Internet Safety Awareness Week, information and education will also be provided for our parents.

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with in line with our Promoting Positive Behaviour Policy, Anti Bullying Policy and our Safeguarding and Child Protection Policy.

Pupils are made aware that any misuse of mobile/phones/websites/emails should be reported to a member of staff immediately.

School Twitter Account

The school operates a private twitter account to provide information and reminders to parents/carers and governors, to promote the school and to celebrate pupils' work. Parents are encouraged to join through the newsletter and meetings but they must send a request and then be accepted. To safeguard the interests of pupils, photographs will be selected carefully. Only pupils whose parents have given written permission will be tweeted. We also ask permission from the children. Pupils' names will not be tweeted.

Management of Personal Data

Personal data that is stored in SIMS and the intranet is password protected. Staff are aware of the importance of keeping passwords private so that pupil and staff data is kept secure. The school maintains a Register of Access which outlines who has access to the different pupil and staff information stored on the school system, based on user need.

Links to other policies

This policy should not be seen in isolation and should be read in conjunction with the Safeguarding and Child Protection Policy, the Promoting Positive Behaviour Policy, the Anti-Bullying Policy and the Staff Code of Conduct.

Monitoring and Review

This policy will be reviewed annually or after any breaches or potential breaches of online safety. The ICT coordinator records any breaches/potential breaches in an Online Safety Risk Register and subsequent actions.

Appendices

1. Code of Practice for Pupils
2. Code of Practice for staff
3. Parent Consent letter
4. Online Safety Curriculum Overview
5. Ipad Acceptable Use Policy for School Staff