St. Cecilia’s Catholic Infant and Nursery School

Online/E-Safety Policy

Development/ Monitoring and Review of this Policy

This Online/ E-Safety policy has been developed by a working group made up of:

- School E-Safety Coordinator
- Headteacher
- Teachers
- Governors

Consultation with the whole school community has taken place through

- Staff meetings
- Governors meeting
- School website / newsletters

Due to the ever changing nature of Information and Communication Technologies, we will review the e-safety Policy annually or, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Scope of the Policy

Through our Online/ E-safety policy, we aim to meet our statutory obligations to ensure that children, staff and visitors are safe and are protected from potential harm.

This policy:

- Identifies the key people and their roles and responsibilities.
- Outlines the strategy in which the school will endeavor to keep its pupils safe from harm, both by electronic protection, and by education of pupils and parents
- Identifies the procedures to follow in the case of an incident

This Online/e-safety policy is used in conjunction with other school policies including Behaviour, Anti-bullying and Child protection policies that help to address both online and offline behaviours.

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Roles and Responsibilities

The Appointed Online/E-Safety Governor Mrs A Billing

Their role includes:

- Meeting with the Online/E-Safety Co-ordinator on a regular basis
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors committee meetings

The Designated Online/E-Safety Coordinator – Mrs E Rhodes / Mrs E van de Waal

Their role includes the following:

- Leading the school Online/e-safety committee
- Day to day responsibility for Online/e-safety issues with a leading role in establishing and reviewing the school e-safety policies and documentation
- Ensuring that all staff are aware of the policy and the procedures that need to be followed in the event of an online/e-safety incident taking place.
- Providing training and advice for staff
- To liaise with the Local Authority and other agencies if and when required
- To work with school ICT technical staff on e-safety
- To receive reports of online/e-safety incidents and maintain a log of incidents to inform future online/e-safety policy and practice
- To meet regularly with E-Safety Governor to ensure Governing body is kept aware of current practice

Headteacher and Senior Leaders:

The Headteacher has overall responsibility for ensuring the safety of members of the school community. However, the day-to-day responsibility for online/e-safety will be delegated to the Online/E-Safety Co-ordinator. The SLT will receive regular monitoring reports from the online/E-Safety Co-ordinator and attend the regular meeting as part of the online/E-Safety Meeting

The Designated person for child protection – Mrs S MacGregor

They will work with the online/E-Safety Co-ordinator drawing on each other's experience and expertise in order to ensure that pupils are kept safe, and should be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Online/E-Safety Committee

The Following people make up the e-safety committee and shall meet every half term to discuss the Online/E-safety Co-ordinators report
Headteacher
SMT Rep
Teaching Assistant Rep
Child Protection Co-ordinator

Pupils

Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy and should understand the importance of adopting good online/e-safety practice when using digital technologies out of school and realise that the school's online/e-safety Policy covers their actions out of school, if their actions have an impact upon school

Parents & Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. They should sign the Pupil Acceptable Use Policy.

Context:

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience; it is a part of the statutory curriculum and a necessary tool for staff and pupils.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and effective curriculum practice;
- communication and collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and LDL;
- access to learning wherever and whenever convenient.

Assessing risks

Although we recognise the benefits of technology we must also be aware of the potential risks, which may include:

- Access to illegal, harmful or inappropriate images or other content (including video / games)
- Unauthorised access to / loss of / sharing personal information
- Inappropriate communication / contact with others (including strangers)
- Cyberbullying
- The risk of being subject to grooming by those with whom they make contact on the Internet
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Copyright infringement – including plagiarism, illegal downloading of music / video

The benefits to pupils from access to the resources on the internet far outweigh the disadvantages. The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor RCC can accept liability for any material accessed, or any consequences of Internet access.

Methods to identify, assess and minimise risks will be reviewed regularly. The Headteacher will ensure that the online/e-Safety policy is implemented and compliance with the policy monitored.

The responsibility for setting and conveying the standards that children are expected to follow, when using the internet, is one which the school shares with parents/carers.

Online/E-Safety Education

Education for Pupils

The resources used by pupils in our school are usually carefully chosen by the teacher and determined by curriculum policies. The Internet, by its very nature is different. Children will have access to information, which at times has not been selected by the teacher. Whilst pupils will usually be directed to sites that have been previously evaluated by teachers, there will be times when children will be able to move away from these 'familiar' sites to areas that are unfamiliar to the teacher and children.

Keeping children safe online is critically all about education. Although filters are in place to protect pupils whilst in school, this is only a small percentage of the time that a child is potentially on-line. There may not be such filtering in the 'home' environment.
School will educate pupils in how to negotiate the Internet without the safety net of filtering in place. This is the same principle Stranger-Danger and Road Safety - developing risk strategies and responses to threats – potential or real.

The School will provide online/E-Safety education in the following ways:

- A planned online/e-safety programme as part of ICT / PHSE / other lessons, with key themes regularly revisited covering all communication technologies where there is a safety risk
- Key online/e-safety messages should be reinforced in assemblies (with parents invited to share)
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils should be taught in all lessons to be critically aware that not everything they access on-line is truthful or valid
- Pupils will be taught to report anything that upsets them on-line to a trusted adult
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils will be encouraged to adopt and promote safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT systems and the internet will be posted in all rooms regardless of if computers are in use there, as the use of mobile devices means that the Internet is accessible across the site, and will be discussed with the pupils regularly.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education for Parent & Carers / Enlisting support

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home. Parents are also advised to check if pupils' use elsewhere, such as libraries, is covered by an appropriate use policy.

- Parents'/Carers' attention will be drawn to the school's online/e-safety Policy in newsletters, the school brochure and on the school website.

- Internet issues will be handled sensitively, and parents/carers will be advised accordingly.
- A partnership approach with parents will be encouraged.
- The school will maintain a list of online/e-Safety resources for parents/carers.
- The school will ask new parents to sign the parent/pupil agreement when they register their child within the school.

Education & Training for Staff

All staff should receive online/e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online/e-safety training will be made available to staff. An audit of the online/e-safety training needs of all staff will be carried out regularly.
- All new staff should receive online/e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The School will seek to provide the best advice on practice to support E-Safety training as required to individuals and groups

Training for Governors

- Governors should undertake e-safety training / awareness sessions both individually for nominated persons, and as a body, in order to discharge its responsibilities as in the 2012 OfSTED Handbook

Acceptable Use Policies

The school has adopted the Liverpool Authority Acceptable Use of ICT Policy. (See Appendix)

All staff, parent helpers, volunteers and pupils (with their parents/carers) will be asked to read and sign an agreement covering the expectations we have of users using the internet in school.

AUP for pupils MUST be signed by both pupils and parents and returned to school on entry to the school. If parents change their minds about their child's use of the internet they need to inform the school in writing.

Any person not directly employed by the school will be asked to sign an 'Acceptable use of ICT' policy before being allowed to access the internet from the school site.

Managing Internet Access in the School

The school's educational network and access to the Internet is provided by Liverpool City Council through its IT partner Liverpool Direct Limited (LDL).

The school maintains a current record of all staff and pupils who are granted access to the school's ICT systems. All users should be aware that periodic monitoring of internet traffic may take place to ensure that responsible school use of the internet is maintained.

Filtering

- The school works in partnership with parents, the LA, LDL and MGL to ensure that systems to protect pupils are reviewed and improved.

- The school internet access is designed expressly for pupil use and has a multi-layer security shield that provides dual layer firewall protection, intruder detection / prevention, load balancing, content-caching, data traffic analysis and virus protection. There is a cloud-based filtering service, ScanSafe, which filters Internet content using the City Council's base policy, and live scans all sites to block any threats or inappropriate websites.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- iPads have restrictions enabled.
- Staff will use a child friendly safe search engine when accessing the web with pupils.

Reporting Procedures

Despite all attempts of filtering, pupils may be subjected to inappropriate material wherever they can access the Internet. Pupils need to be made aware of the procedure to follow if they come across something they deem as being inappropriate / upsetting.

- Pupils report to a trusted adult – they switch off the monitor / close laptop lid / close iPad sleeve – they should not turn off the machine.
- Staff need to report the URL (address) of unsuitable sites to the E-Safety coordinator, who will then pass this information onto the LEA internet service provider. Any material that the school believes is illegal must be reported to appropriate agencies such as the Internet Watch Foundation (IWF) or CEOP: Child Exploitation and Online Protection Centre.

E-Security

The School will take all reasonable steps to maintain a safe and secure environment

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media, such as memory sticks and CD-ROMs, may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

E-mail / Digital Communication

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, e-mail is not considered private and is monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

- Pupils may only use approved e-mail accounts on the school system.
- Whole class or group email will be used with pupils.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Pupils may not access personal email accounts in school.
- E-mail sent to an external organisation is 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.
- The sending of abusive or inappropriate email messages is forbidden.

The School Website

The school web site – www.stceciliasinfants.org.uk - celebrates pupils' work and promotes the school.

- The point of contact on the Web site is the school address, school e-mail and telephone number. Staff or pupils' personal information is not published.
- The Headteacher and ICT Co-ordinator take overall editorial responsibility and try to ensure that content is accurate and appropriate.
- Photographs that include pupils are selected carefully.
- Pupils' full names are not used anywhere on the Web site or other online space, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are electronically published.
- Work can only be published with the permission of the pupil and parents/carers.
- The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social Networking and Personal Publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Safeguarding Policy

For more information about how we deal with any safeguarding issue in school, please refer to the Safeguarding Policy

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.
- The senior management team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school has adopted the Data Retention Policy for Liverpool Schools.

Unsuitable / Inappropriate Use

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to anything of an illegal, criminal, obscene, inappropriate, racist, threatening nature.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

Responding to Misuse

- Any incidents will be logged on the school Online/E-Safety Incident Log (see appendix)
- Prompt action is required if a complaint regarding the inappropriate use of the Internet is made. The facts of the case need to be established, for instance whether the Internet use was within or outside school.
- Complaints of Internet misuse will be dealt with by a senior member of staff; complaints about staff misuse must be referred to the headteacher.
- Incidents of pupil misuse will be dealt with through normal behaviour and disciplinary procedures as detailed in the School Behaviour Policy. Subsequently access may be denied to internet resources
- Complaints of a child protection nature must be referred the school Designated Child Safeguarding Coordinator and dealt with in accordance to school child protection procedures
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with other safeguarding issues, there may be occasions when the police must be contacted.