Our Lady of Lourdes Catholic Primary school

eSafety Policy

(Adapted from the London Borough of Enfield's 'Education E-Safety Policy Guidance')

Mission Statement

Our Parish School of Our Lady of Lourdes
welcomes everyone in the community,
to share with us the joys of our Catholic Faith.
We worship, learn and play together in the love of Jesus,
helping one another to become the people
God has created us to be.

School eSafety Policy

The school's designated Child Protection Officer will also act as the eSafety coordinator as these roles overlap. At Our Lady of Lourdes School the designated Child Protection Officer is the Headteacher.

Our eSafety Policy has been written by the school, building on the London Borough of Enfield's eSafety guidance.

This eSafety Policy will be reviewed regularly by the Governing Body.

What is eSafety?

e-Safety reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

e-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones, handheld devices and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Children must also learn that publishing personal information could compromise their security and that of others.

At Our Lady of Lourdes School it is made clear to children, staff and visitors, through our programme of eSafety and the use of Acceptable Use Policies, that the use of school equipment for inappropriate reasons is "unauthorised". This policy also details other ways the school works to ensure that all reasonable actions have been taken and measures put in place to protect users.

Our School's eSafety Policy operates in conjunction with other school policies including Behaviour, Child Protection and Anti-Bullying.

Why is Internet use important?

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 functions.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st Century life for education, business and social interaction. Access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access as it is an essential part of their learning experience.

Pupils 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.

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's Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of the pupils;
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use;
- The School will endeavour to ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the correct use of published material and taught to understand and respect copyright and intellectual property rights;
- Internet access will be planned to enrich and extend learning activities;
- Staff will guide pupils in online 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;
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

How will Management Information Systems be maintained?

- The security of School Management Information Systems will be reviewed regularly;
- Virus protection will be updated regularly;
- Security strategies will be discussed;
- Personal data sent over the Internet will be encrypted or otherwise secured;
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998;
- Portable media 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 email;

- Files on the school's network will be regularly checked;
- The Computing subject leader and Office Manager will review system capacity regularly for the curriculum and admin networks respectively.

How will email be managed?

- Pupils may only use approved e-mail accounts on the school system. These will be either whole-class or group email accounts;
- Pupils must immediately tell a teacher if they receive offensive email;
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission;
- Access in school to external personal email accounts may be blocked;
- Email 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;
- Staff should not use personal email accounts for professional purposes.

How will published content be managed?

- The contact details on the School Website will be the school address, email and telephone number. Staff or pupils' personal information will not be published;
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate;
- The School Website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupils' images or work be published?

- Images (both still and moving) that include pupils will be selected carefully to be published and pupils will not be identified by name;
- Written permission from parents or carers will be obtained before images and/or work of pupils are electronically published.
-

Social networking

- Where feasible, the school will 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 will be advised not to place personal photos on any social network space;
- Pupils will 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.

Internet access and filtering

All pupils, prior to receiving Internet access, will be taught how to use the system responsibly and will be made aware of our Acceptable Use Policy for Children.

In common with other media such as magazines, books and video, some material available via the Internet is inappropriate for pupils. Inappropriate material includes pornography, information relating to the misuse of drugs and the promotion of violence, intolerance, racism and extreme political and social views. Pupils in School are unlikely to see inappropriate content in books due to selection by publisher and teacher and the School will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. The following measures have been adopted to help ensure that our pupils are not exposed to inappropriate material:

- our Internet Service Provider (ISP) provides a filtered service which examines the content of web pages for inappropriate material;
- children using the Internet will be supervised by a member of staff at all times;
- staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of the pupils;
- staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan; pupils will be informed that checks can and will be made on files held on the system and the sites they access;
- pupils will be taught to use email and the Internet responsibly in order to reduce the risk to themselves and others;
- our Rules for Responsible Internet Use will be displayed in the ICT suite;
- our Acceptable use statement for staff and governors will be displayed in the ICT suite;
- the School will work in partnership with parents, the LA, the DCSF and our ISP to ensure systems to protect pupils are reviewed and improved.

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that inappropriate material will never appear on a computer terminal or tablet device. ***Neither the School nor the LA can accept liability for the material accessed, or any consequences thereof.***

An important element of our Rules for Responsible Internet use is that pupils will be taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material the School will wish to respond to the situation quickly. Our first priority will be to give the pupil appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the School has taken.

If staff or pupils discover inappropriate sites the URL (website address) will be reported to the Computing subject leader. The Computing subject leader will report this to our ISP and the LA; if it is thought the material is illegal, after consultation with the ISP and LA, the site will be referred to the Internet Watch Foundation and the police.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules for Responsible Internet Use which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet or use of email facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when given the privilege of undertaking their own Internet search, then sanctions consistent with our own School Behaviour Policy will be applied. Teachers may also consider whether access to the Internet may be denied for a period.

All members of the School community have a responsibility to ensure that pupils experience safe Internet access both in School and at home.

The School aims not only to support parents whose children have access to the Internet at home, but those parents who may be concerned about safe access to the Internet. The School aims to support parents in a number of ways:

- the Computing subject leader is willing to offer advice and suggest alternative sources of advice on the understanding that neither he/she, the School or the LA can be held responsible for the consequences of such advice;
- the Computing subject leader will maintain a stock of relevant leaflets from organisations such as PIN and NCH Action for Children;
- a copy of the School's eSafety Policy will be available for parents to read on the School website;
- parents will be kept informed of any future ICT developments through the School newsletter.

As outlined in this policy, teachers have a responsibility to teach their pupils the Rules for Responsible Internet Use and the reasons for these rules before allowing access to the Internet. Along with other staff, teachers must abide by the Acceptable use policy for staff and governors (See Acceptable Use Policies), and ensure that any student teachers they are hosting are aware of these statements, and our eSafety Policy. All staff must read and sign the Acceptable use statement before using any school ICT resource.

Any abuse of the School computer system by any member of the School community may result in disciplinary action being taken and, in extreme circumstances, police intervention.

Videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet;
- Videoconferencing will only take place under the guided supervision of the class teacher.

Emerging technologies

- Emerging technologies will be examined for educational benefit and potential risks before use in school is allowed;
- Staff will be issued with a school mobile phone where contact with pupils or parents is required (e.g. on a residential trip);
- Children in Year 6 who are authorised to go home alone may bring in a mobile phone in the Summer term. During the school day the mobile phone is secured safely in the School Office. It is the child's responsibility to collect the mobile phone at the end of the school day.

eSafety 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 Headteacher;
- Parents wishing to make a complaint about an eSafety issue should use the established school complaints procedure;
- Complaints of a Child Protection nature must be dealt with in accordance with Child Protection procedures.

Cyber bullying

- Along with all other forms of bullying, Cyber bullying will not be tolerated in school. See anti-bullying policy;
- There will be clear procedures in place to support anyone effected by cyber bullying;
- All incidents of cyber bullying reported to the school will be recorded.

Sanctions for those involved in cyber bullying may include:

- The cyber bully being asked to remove any material deemed to be inappropriate or offensive;
- A service provider may be contacted to remove content;
- Internet access may be suspended at school for the user for a period of time;
- Parents / Carers will be informed;
- The police will be contacted if a criminal offence is suspected.

How will the policy be introduced to pupils?

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored;
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use;

- Instruction in responsible and safe use should precede Internet access.

How will the policy be discussed with staff?

- All staff will be given access to the School E-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's E-Safety Policy in the school newsletter and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to relevant organisations and the school will endeavour to periodically offer parents an eSafety workshop.

Legal Framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.
- *Some of the legislative acts noted below have amendments pending*

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).
- UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.