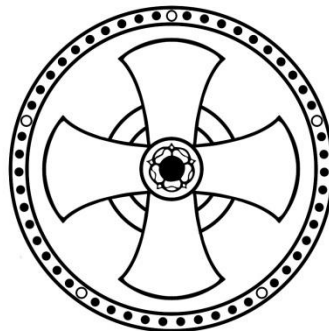Our Lady of Lourdes Catholic Primary School

E-Safety Policy

Reviewed February 2015

Live
Love
Learn

Our Lady of Lourdes Primary School
E-Safety Policy

Contents

Page

Our Lady of Lourdes Primary School
E-Safety Policy

SCHOOL MISSION STATEMENT

Our purpose is to live, love
and learn
as a school community
in partnership with home,
parishes and the wider world.

We place our faith in God,
And the Gospel Values of His Son,
Jesus Christ,
At the centre of all we do.

We come together
as witnesses to His example;
to serve, to challenge
and to encourage growth
into all that we are created to be.

Each individual shares
in the role of teacher and learner.
We rejoice in, and celebrate
all our achievements and uniqueness,
as a family.

Our Lady of Lourdes Primary School
E-Safety Policy

Pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Schools must decide on the right balance between controlling access, setting rules and educating students for responsible use. Parents and schools must develop complementary strategies to ensure safe, critical and responsible ICT use wherever the young people may be.

The school will appoint e-Safety coordinators. These will be both the designated Child Protection persons and the ICT coordinator. Our E-Safety Policy has been written by the school, building on Government guidance. It has been agreed by the senior management team and approved by governors. The E-Safety Policy will be reviewed annually.

This policy applies to:

Pupils
All school staff
Governors
All adults who carry out roles in school in any position of trust

AND, for adults listed above, the policy refers to their information technology behaviour and activity outside of the school ICT systems, particularly with or in reference to any other individuals who fall within the list above. Please see section below: Staff, Governors and Other Adult Guidance.

STAFF, GOVERNORS AND OTHER ADULT GUIDANCE

Adults in contact with pupils in the school must follow core principles:

You are accountable for your own ICT behaviours at all times, whether through school or private ICT systems, and should use your best judgment to avoid at

Our Lady of Lourdes E-Safety Policy
Reviewed February 2015
Next Review February 2016

Our Lady of Lourdes Primary School
E-Safety Policy

all times inappropriate e-contact with pupils, past and present, and their parents.

No non-school ICT e-contact with pupils, past or present who are under the age of 18, may be deemed appropriate, unless expressly authorised by the Head or governing body in exceptional circumstances.

Your private and school e-communications should reflect that you have a position in the school.

You should keep aware that your e-communications may be the subject of scrutiny by the school and other authorities if it is felt that they contravene this policy, or bring the school into disrepute.

Online Social Networking for adults

The Department for Children, Schools and Families (DCSF) has published guidance on social networking sites. The school supports the advice given to teachers in this guidance, and draws attention to the following comments on page 6:

'When publishing information, personal contact details, video or images, ask yourself if you would feel comfortable about a current or prospective employer, colleague, pupil or parent, viewing your content.'

When using any social networking sites, such as 'Facebook', staff, governors and other adults referred to in this policy SHOULD NOT, for example, accept or initiate friendship requests from pupils past or present who are under the age of 18, or parents of children currently at the school. Staff and governors should also examine and adjust the security settings carefully to allow only 'friends' to access personal photos and information. On rare occasions, the governing body may approve such contact referred to in this paragraph by staff member, governor or other adult referred to, on application to the governing body directly by the that individual.

<u>Acceptable Use Statement (also in ICT policy)</u>

The computer system is owned by the school, and may be used by children to further their education and by staff to enhance their professional activities including teaching, research, administration and management.
The school recognises that technologies such as the Internet and e-mail will have a profound effect on children's education and staff professional development in the coming years and the school's E-Safety Policy and Acceptable use Policy have been drawn up accordingly.
The installation of software or hardware unauthorised by the school, whether legitimately licensed or not, is expressly forbidden.
The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.

<u>Acceptable use of the internet and email systems</u>

Our Lady of Lourdes Primary School
E-Safety Policy

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 pupils. Pupils must also learn that publishing personal information could compromise their security and that of others.

Using the internet

• All Internet activity should be appropriate to staff professional activities or the children's education;

• Pupils must be supervised at all times when using the Internet. All staff should be aware that networked computers are generally online at all times when a user is logged on.

• Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;

• Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited;

• Use for personal financial gain, political purposes or advertising is excluded;

• Copyright of materials must be respected;

• The use of the Internet, e-mail, or any other media to access inappropriate materials is expressly forbidden.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access on school ICT systems.
- New pupils and staff will be made aware of the e-safety rules of the school and sign the necessary consent forms to access the internet.
- All staff, Governors, and visiting teachers 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 form for pupil access.
- The school will maintain settings on the school ICT system to limit access to inappropriate material on the internet, wherever possible.

Our Lady of Lourdes Primary School
E-Safety Policy

For our pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. If pupils access inappropriate materials teachers/teaching assistants should…

• Close or minimise the image or window immediately. Don't try to navigate away.
• If pupils saw the page, talk to them about what has happened, and reassure them.
• Later, investigate the history of visited sites and how the pupil got there.
• Inform the ICT coordinator who will in turn inform the head and contact the schools ICT helpdesk.

Our Lady of Lourdes Primary School
E-Safety Policy

<u>Using Email</u>

• For external e-mail, there is no need for pupils to use individual accounts. A 'class' e-mail address may be set up, and moderated by the teacher.

• Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media;

• Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;

• The use of the Internet, e-mail, or any other media to access inappropriate materials is expressly forbidden.

'Netiquette'

Staff and students need to understand that the use of the school's network is a privilege which can be removed should a good reason arise. The school may monitor all network and Internet use in order to ensure student safety.

All users should be expected to adhere to the generally accepted rules of network etiquette.

These include but are not limited to the following:

_ *Be polite.*

_ *Use appropriate language.*

_ *Do not use abusive language in your messages to others.*

_ *Do not reveal the address, phone number or other personal details of yourself or other users.*

_ *Do not use the network in such a way that would disrupt the use of the network by other users.*

_ *Illegal activities are strictly forbidden.*

_ *Note that e-mail is not guaranteed to be* private.

_ System administrators monitor and have access to all e-mail.

_ Messages relating to or in support of illegal activities may be reported to the authorities.

Our Lady of Lourdes Primary School
E-Safety Policy

Internet Publishing Statement (using pupil images and recordings)

The school wishes the school's web site/learning platform to reflect the diversity of activities, individuals and education that can be found at Our Lady of Lourdes Catholic Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles should be borne in mind:

• Parents will be asked at the beginning of each year for permission to publish photos, audio recordings (podcasts) and videoed materials of children on the website/learning platform.

• All staff must be familiar with who can and can't have pictures taken for the internet or recordings made. Lists of these can be provided by the office or ICT coordinator.

• No recording (audio or visual) will be published without the child's own verbal consent.

• Names of children will not be published, especially in conjunction with photographic or video material.

• No link should be made between an individual and any home address (including simply street names).

• Pupils should not upload photographs or videos of themselves or other pupils.

• Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in doubt, refer to the person responsible for child protection.

Our Lady of Lourdes Primary School
E-Safety Policy

Cyber bullying

This school believes that all people in our community have the right to teach and learn in a supportive, caring and safe environment without fear of being bullied. We believe that every individual in school has a duty to report an incident of bullying whether it happens to themselves or to another person.

WHAT IS CYBER-BULLYING?

There are many types of cyber-bullying. Although there may be some of which we are unaware, here are the more common.

1. Text messages —that are threatening or cause discomfort - also included here is

"Bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)

2. Picture/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.

3. Mobile phone calls — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.

4. Emails — threatening or bullying emails, often sent using a pseudonym or somebody else's name.

5. Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based Chatroom.

6. Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger) or Yahoo Chat – although there are others.

7. Bullying via websites — use of defamatory blogs (web logs), personal websites, the school's learning platform and online personal "own web space" sites such as Bebo, Facebook and Myspace (although there are others).

At Our Lady of Lourdes Primary School, we take this bullying as seriously as all other types of bullying and, therefore, will deal with each situation individually. An episode may result in a simple verbal warning. It might result in a parental discussion. Clearly, more serious cases will result in further sanctions.

Technology allows the user to bully anonymously or from an unknown location, 24 hours a day, 7 days a week. Cyber-bullying leaves no physical scars so it is, perhaps, less evident to a parent or teacher, but it is highly intrusive and the hurt it causes can be very severe.

9

Our Lady of Lourdes Primary School
E-Safety Policy

Young people are particularly adept at adapting to new technology, an area that can seem a closed world to adults. For example, the numerous acronyms used by young people in chat rooms and in text messages (POS - Parents Over Shoulder, TUL – Tell You Later) make it difficult for adults to recognise potential threats.

At Our Lady of Lourdes Primary School, pupils are taught how to:

• Understand how to use these technologies safely and know about the risks and consequences of misusing them.

• Know what to do if they or someone they know are being cyber bullied.

• Report any problems with cyber bullying.

Our Lady of Lourdes Primary School has:

1. An E-Safety policy (this document) that includes clear statements about e-communications

2. Information for parents on: E-communication standards and practices in schools, what to do if problems arise, what's being taught in the curriculum (see the school website).

3. Support for parents and pupils if cyber bullying occurs by: assessing the harm caused, identifying those involved, taking steps to repair harm and to prevent recurrence

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 phone where contact with pupils is required.

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.
- All staff to sign the Acceptable Use Policy.
- 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, the school brochure and on the school Web site.

E-safety co-ordinator

- It is the role of the e-safety co-ordinator to maintain up to date records of information generated by this policy.

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 headteacher.

- Complaints of a child protection nature will 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.

Our Lady of Lourdes Primary School
E-Safety Policy

Pupil Advice

If you're being bullied by phone or the Internet remember, bullying is never your fault. It can be stopped and it can usually be traced.

• Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.

• Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.

• Don't give out your personal details online - if you're in a Chatroom, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.

• Keep and save any bullying emails, text messages or images. Then you can show them to a parent or teacher as evidence.

• If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

• There's plenty of online advice on how to react to cyber bullying. For example,

• www.kidscape.org and www.wiredsafety.org have some useful tips: Text/video messaging

• You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit If the bullying persists, you can change your phone number. Ask your mobile service provider.

• Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying.

• Visit their website for details.

• Don't delete messages from cyber bullies. You don't have to read them, but you

• should keep them as evidence.

• Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer.

If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls

Our Lady of Lourdes Primary School
E-Safety Policy

If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off.

Once they realise they can't get you rattled, callers usually get bored and stop bothering you.

1. 1 Always tell someone else: a teacher, youth worker, parent, or carer. Get them to support you and monitor what's going on.

2. Don't give out personal details such as your phone number to just anyone.

3. Never leave your phone lying around. When you answer your phone,

4. Just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not.

5. You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.

6. Don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again.

7. Almost all calls nowadays can be traced. If the problem continues, think about changing your phone number.

8. If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

Emails

• Never reply to unpleasant or unwanted emails ('flames') — the sender wants a response, so don't give them that satisfaction.

• Keep the emails as evidence. And tell an adult about them.

• Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com

• Never reply to someone you don't know, even if there's an option to 'unsubscribe'.

• Replying simply confirms your email address as a real one.

Web bullying

• If the bullying is on a website (e.g. Bebo) tell a teacher or parent, just as you would if the bullying were face-to-face – even if you don't actually know the bully's identity.

Our Lady of Lourdes Primary School
E-Safety Policy

• Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging

• Never give out your name, address, phone number, school name or password online.

• It's a good idea to use a nickname.

• Don't give out photos of yourself.

• Don't accept emails or open files from people you don't know.

• Remember it might not just be people your own age in a chat room.

• Stick to public areas in chat rooms and get out if you feel uncomfortable.

• Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.

• Think carefully about what you write; don't leave yourself open to bullying.

• Don't ever give out passwords to your mobile or email account.

Three steps to stay out of harm's way

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.

2. If someone insults you online or by phone, stay calm – and ignore them.

3. 'Do as you would be done by.' Think how you would feel if you were bullied.

4. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.

The law is on your side

The Protection from Harassment Act, the Malicious Communications Act 1988

And Section 43 of the Telecommunications Act may be used to combat Cyber bullying. People may be fined or sent to prison for up to six months.

Our Lady of Lourdes Primary School
E-Safety Policy

PRECEDENT LETTER FROM STAFF/GOVERNORS TO THE GOVERNING BODY TO REQUEST PERMISSION FOR SOCIAL MEDIA CONTACT WITH PARENTS OF PUPILS AT THE SCHOOL.

Dear Governing Body

I have read the E Safety and Acceptable Use policies of Our Lady of Lourdes School, and I acknowledge that my role as [   ] falls within these policies and I am, therefore, obliged to adhere to these policies at all times. I also acknowledge that the E Safety policy refers to contact via social networking with parents and pupils, and prohibits such contact, unless authorised by the governing body.

I ask the governing body to note that from time to time I [may] have contact via such networking sites with parents with whom I have a personal or other social reason for such contact. I confirm to the governing body that any such contact I have nevertheless adheres to the policy in every other respect.

I therefore request that the governing body agree to my continued contact with such parents via social media and I confirm that at all times my contact will adhere to the spirit and aims of the policies.

I understand that the governing body may request further details from me regarding such contact and may review their decision and withdraw permission at any time.