Our Lady of Lourdes Catholic Primary School

Online Safety Policy			
Date	**Review Date**	**Coordinator**	**Nominated governor**
September 2020	September 2022	James Green	Bernard Arscott (Safeguarding portfolio holder)

Mission Statement

Loving like Mary
Serving like Mary
Learning like Mary
Believing like Mary

1. Policy Statement

This policy is to ensure that all pupils and adults at Our Lady of Lourdes understand the importance of Online Safety and know how to keep themselves and sensitive information safe when using IT.
This policy applies to all members of the Our Lady of Lourdes community who have access to and are users of school IT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The Safeguarding Policy should be referred to when there are any child protection concerns.

Online Safety and the maintaining of data securely is everyone's responsibility - whether they are a pupil, member of staff, a parent or a governor. Failure to apply agreed controls to secure data can be a serious matter, even resulting in legal action.

Further information is available at the following sites (those marked with a * are particularly useful for parents:

https://www.thinkuknow.co.uk/ *
https://ceop.police.uk/safety-centre/
http://www.iwf.org.uk/
http://educateagainsthate.com/
https://www.saferinternet.org.uk/ *
https://www.commonsensemedia.org/ *
https://www.internetmatters.org/ *

https://www.disrespectnobody.co.uk/ *
NB: This policy must be read in conjunction with Appendix C KCSIE (Sept 2020)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/892394/Keeping_children_safe_in_education_2020.pdf

Where children are being asked to learn online at home then Coronavirus: safeguarding in schools, colleges and other providers and Safeguarding and remote education during coronavirus should be referred to.

2. Definitions
Online Safety: procedures to ensure all members of the school community know their access rights and responsibilities in using IT.

Online Security: procedures to protect the physical network infrastructure to ensure all information and electronic data is securely maintained and is categorised as public, protect or restricted.

3. Aims and Objectives

The purpose of this policy is to:
▪ set out the key principles expected of all members of the school community with respect to the use of IT-based technologies;
▪ safeguard and protect all pupils and staff;
▪ assist staff working with pupils to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice;
▪ set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community;
▪ have clear structures to deal with online abuse such as online bullying;
▪ ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken; and
▪ minimise the risk of misplaced or malicious allegations made against staff.

4. What are the main areas of risk?

The main areas of risk for our school community are summarised below:

4.1 Content
■ Exposure to inappropriate content
■ Lifestyle websites promoting harmful behaviours
■ Hate content
■ Content validation (how to check the authenticity and accuracy of online content)

4.2 Contact

■ Grooming (sexual exploitation, radicalisation, gang culture etc.)
■ Social or commercial identity theft, including passwords
4.3 Conduct
■ Aggressive behaviour
■ Online bullying or harassment
■ Privacy issues, including hacking or disclosure of personal information
■ Digital footprint and online reputation
■ Health and wellbeing (time spent online, gambling, body image)
■ Sexting
■ Copyright

5. Roles and Responsibilities

Role Key Responsibilities

Head Teacher (and SLT)
■ To lead a safeguarding culture, ensuring that online safety is fully integrated with whole school safeguarding.
■ To take overall responsibility for online safety provision.
■ To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling.
■ To ensure the school uses appropriate IT systems and services including, filtered Internet Service e.g. LGfL services.
■ To be responsible for ensuring that all staff receive regular training to carry out their safeguarding and online safety roles, including as part of induction.
■ To be aware of procedures to be followed in the event of a serious online safety incident.
■ To ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils.
■ To ensure there is a system in place to monitor and support staff who carry out internal online safety procedures.
■ To ensure governors are updated on the nature and effectiveness of the school's arrangements for online safety.

Computing & Online Safety Leader
■ To take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy.
■ To promote an awareness and commitment to online safety throughout the school community.
■ To liaise with technical support where appropriate.
■ To remain updated in online safety issues and legislation, and be aware of the potential for serious safeguarding concerns.
■ To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident, including logging any safeguarding concerns.
■ To facilitate training and provide advice to all staff.

■ To ensure that Online Safety education is embedded in the curriculum.
■ To ensure the school website is up to date and includes all required information.
Network Manager/ Technical Support Staff
■ To report online safety related issues that come to their attention.
■ To manage the school's computer systems, ensuring- systems are in place for misuse detection and malicious attack e.g. keeping virus protection up to date
- access controls/encryption exist to protect personal and sensitive information held on school devices
- the school's policy on web filtering is applied and updated regularly
■ To keep up to date with the school's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
■ To ensure that the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Head Teacher.
■ To ensure appropriate backup procedures and disaster recovery plans are in place.
■ To keep up to date documentation of the school's online security and technical procedures.

Governors
■ To be aware of the school's approach to online safety.
■ To ensure the school has in place policies and practices including appropriate filters and monitoring systems to keep the children and staff safe online, by attending relevant training, asking questions and receiving reports when appropriate.
■ To support the school in encouraging parents and the wider
community to become engaged in online safety activities.

Data and Information Managers (Asset Owners)
■ To ensure that the data they manage is accurate and up to date.
■ To ensure best practice in information management i.e. have appropriate access controls in place, that data is used, transferred and deleted in line with data protection requirements.
■ The school must be registered with the Information

Commissioner. All staff, volunteers and nominated professionals
■ To embed Online Safety in the curriculum and maintain an awareness of current online safety issues and guidance.
■ To supervise and guide pupils carefully when engaged in learning activities involving online technology.
■ To ensure that pupils are fully aware of research skills and legal issues relating to electronic content such as copyright laws.
■ To read, understand, sign and adhere to the school Acceptable
Usage Agreement, and understand any updates annually (Appendix 1).
■ To report any suspected misuse or problem to the Head Teacher.
■ To model safe, responsible and professional behaviours in their own use of technology.

Exit strategy

■ At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Pupils

■ To read, understand and adhere to the Online Safety Rules and agreement (Appendix 2).

■ To understand the importance of reporting abuse, misuse or access to inappropriate materials.

■ To know what action to take if they or someone they know feels worried or vulnerable when using online technology.

■ To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school.

Parents

■ To read, understand and promote the Online Safety Rules and agreement with their children.

■ To read, understand and sign the use of images letter, notifying the school when there are any changes.

■ To monitor their children's online activity and consult with the school if they have any concerns.

■ To attend workshops and training events provided by the school and its partners.

6. Education and Curriculum

Pupils are encouraged to take responsibility for their own Online Safety, but education in Online Safety forms an essential part of our curriculum. Pupils need help and support to recognise and avoid Online Safety risks and to build their resilience.

Online Safety education is facilitated in the following ways:

■ discussions around Online Safety rules and the need for them so that pupils are encouraged to adopt safe and responsible use in and outside of school;

■ Online Safety sessions across the curriculum, including opportunities for pupil voice;

■ Online Safety awareness in whole school assemblies;

■ lessons where pupils are taught to be critically aware of the materials and content they access online and be guided to validate the accuracy of the information;

■ staff act as positive role models in their use of digital technologies;

■ staff are vigilant when pupils are allowed to search the Internet.

Workshops are provided to parents on occasions so that they are kept informed about Online Safety issues and know how to keep their children safe online.

Youtube:

If a we allow access for pupils or staff, there are three options available from Google:

Open (very high-risk)

This option leaves schools open to accusations of not safeguarding children; it exposes users to every YouTube video, including pornography, graphic violence and more (although these are

against YouTube's terms and conditions). This option is advised against. *No users in our school will have this option available.*

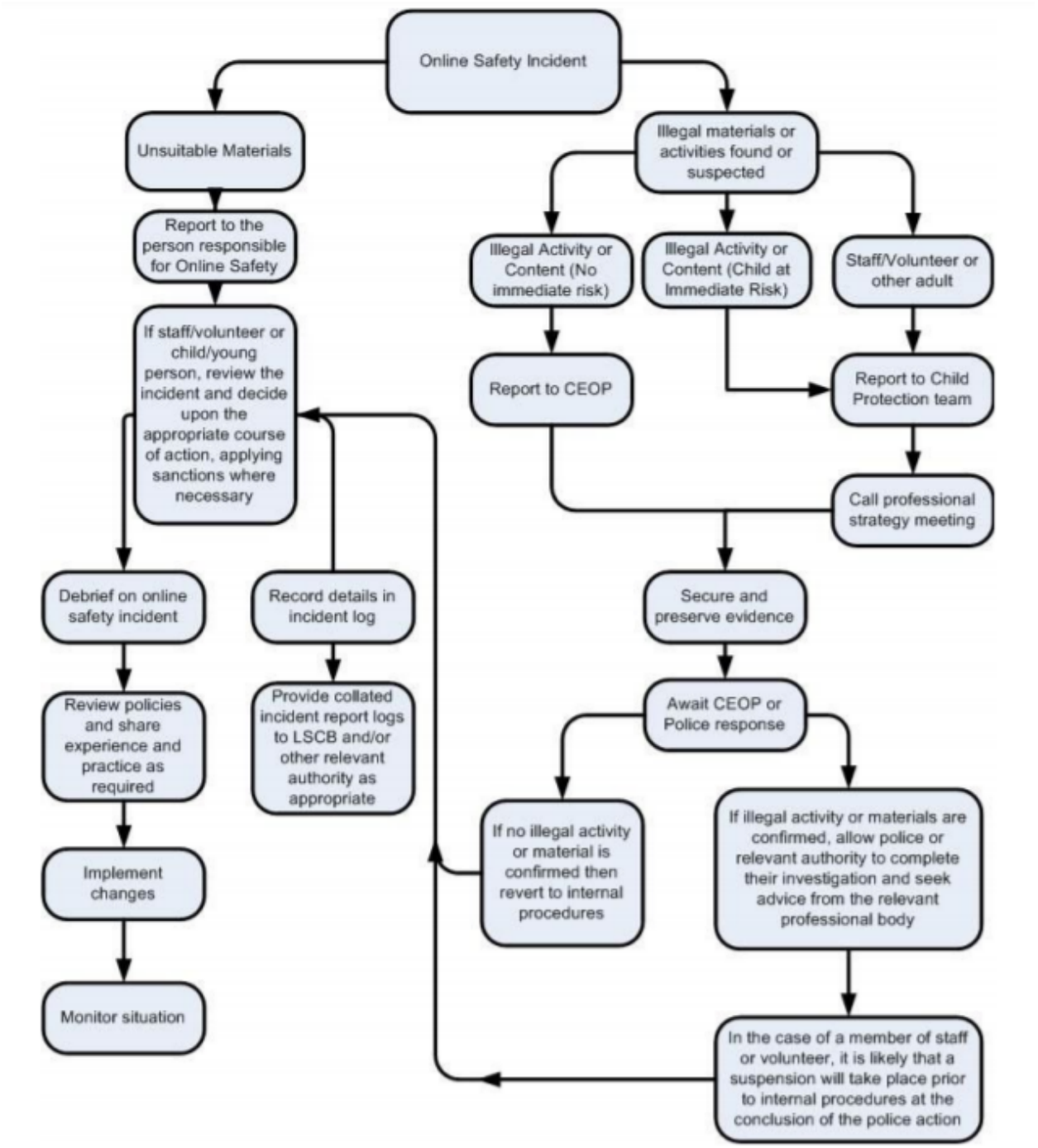
Moderate (restricted mode)
Some schools may find it appropriate to activate this mode, as it is much less restrictive and allows some educational videos which were previously visible but blocked by the severe-restricted mode.
An informed decision to adopt this option should take into consideration that, whilst you are unlikely to ever see sex, pornography, beheadings etc, it does not block keywords. Therefore, you can search 'sex' and view videos on the topic of sex, but these will be largely appropriate for older children. A search for 'pornography' may return advice videos about sexual health, addiction, etc, which might be acceptable for older children, but not for younger ones. Many inappropriate words are used in the title of YouTube channels accessible via this mode e.g. falsely indicating a link to pornography to encourage clicks.
In accordance with the Staff Code of Conduct, specifically use of technology, staff will have access to this option.

Severe-restricted mode (safest, recommended option)
There is always a danger that inappropriate material may be accessed, but it is unlikely due to the highly restrictive version of this mode. Unfortunately, some videos which are clearly educational are blocked.
Pupils at OLOL will have this level of restriction defaulted on their accounts.

7. Incident Management
An important element of Online Safety provision is the ability to identify and manage any incidents that occur. All staff and pupils have a responsibility to report Online Safety incidents so that they may be dealt with effectively and in a timely manner in order to minimise any negative impact. Child protection concerns should be reported in accordance with the Safeguarding Policy; all other incidents should be reported immediately to the Head Teacher, Deputy Head/Assistant Head and/or Online Safety Leader (GH).

The risks relating to Online Safety are caused by people acting inappropriately or illegally. Any issue must be dealt with and observation is essential in being alert to concerns that children may not report. Incidents will vary from pranks or unconsidered actions which may be managed under the school's Behaviour Policy or disciplinary procedures, to occasional incidents that may involve referrals to social care and/or the police.

The following flowchart provides guidance on dealing with concerns:



8. Use of Images

We recognise that photographs and video recordings for school and family use are important, although the potential misuse of images means that everyone has a shared responsibility to ensure that individual and parental rights are respected, and that vulnerable individuals are protected from risk. The taking of photographs or videos at school events is not a breach of the Data Protection Act but due to the potential of inappropriate sharing of images in the community of children and families that do not want

images shared, this is not permitted, and the school will always provide adequately available images for parents to access.

▪ We gain the permission of parents/carers for use of images involving their child on admission in line with our published Use of Images Policy. It is the responsibility of the member of staff taking or publishing the photos to find out about children whose images should not be used. If two parents with parental responsibility disagree over consent, it will be treated that consent has not been given. If parents want to change their decision at any time, they should contact the school.

▪ Parents/carers or unauthorised visitors taking photographs and video recordings is not permitted during normal routines e.g. in classrooms etc. Anyone identified taking unauthorised images of children will be reported to the police.

▪ When images are recorded for school use and/or publication it is important that pupils are suitably dressed and care must be taken during PE lessons, particularly when children are swimming. All images should be screened by the photographer for acceptability and any image that could be used inappropriately should be deleted or destroyed. Images of groups are sometimes more appropriate than individual children, as are images from behind as this makes the children less identifiable. Images should also be inclusive, showing boys and girls from different backgrounds and abilities. In publications where the pictures have captions, it is good practice to only include first names, although local press will often insist on publishing surnames.

▪ Schools keep photographs and video recordings as evidence of children's learning and as a record of school events. Digital images are stored on the school servers, Google drive and on school devices, as well as other cloud based services e.g. Integris, Safeguard, Class Dojo, Tapestry etc. Images of children that have photo consent will be used on the school website; and school twitter/facebook account, though names will not be shared in such cases.

9. Mobile Phones

▪ Mobile phones and other devices brought into school are entirely at the risk of the staff member, pupils, parents and visitors. Schools accept no responsibility for the loss, theft or damage of any phone or device brought into school.

▪ All staff may have a personal mobile phone or other device in their possession at work. However, during lessons and when supervising children, mobile phones should only be used for dialling out in an emergency or receiving calls when an emergency call is anticipated e.g. a sick dependent, a pregnant partner etc. This must be discussed with the member of staff's line manager.

▪ It is acceptable to use mobile phones for school business and whilst on school trips in order to make contact with the school or other adults involved with the trip. It is also acceptable to use a mobile phone in an emergency on the school site where the class radio is not usable.

▪ The recording, taking and sharing of images, video and audio on any personal mobile device is not permitted, except where it has been explicitly agreed by the Head Teacher. If photos are to be published on the school's social media platforms - facebook/twitter or Class Dojo (and parents/carers have given permission), photos *may* be taken live through the relevant app, *but any copy of the photo should be deleted before the end of the school day.*

▪ All mobile device use is to be open to monitoring scrutiny and the Head Teacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary. The school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobile devices may be searched at any time as part of routine monitoring.

▪ It is not advised that staff should contact parents on their personal devices. In the case where a staff member doesn't have access to a school device, they should use their own device and hide their own mobile number for confidentiality purposes.

▪ Pupils are discouraged from bringing mobile phones and other personal devices (e.g. smart watches) into school. However, the school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. This is allowed for Year 6 pupils only. Any year 6 pupil bringing a mobile phone or other device to school must not use it during school hours and must turn their phone off. Phones should be signed in and out of a locker before and after school within the classroom. Pupils must not take photos or use the internet on their phones, and they are not permitted on school trips *under any circumstances*. If a student breaches the policy, then the device will be confiscated and will be held in a secure place until it is collected by a parent/carer.

▪ There may be occasions when personal devices are permitted for pupils, but this must be with the permission of the class teacher and Head Teacher.

10. Remote Access

The use of mobile computing devices and connecting to the school's network from outside of school is increasingly important but presents a number of security risks which need to be addressed. Users of mobile computing facilities (such as laptops) are responsible for safeguarding such equipment and should take all responsible precautions to prevent theft, loss or damage of such items, and to prevent unauthorised access to information held on the device.

The following guidelines apply when accessing systems and information away from the school:
a) Only necessary information should be open/stored on the device.
b) Restricted information shall not be stored on any mobile devices unless password protected.
The removal of any IT equipment, information and software from school premises shall only be permitted with prior authorisation from the Online Safety Leader or Head Teacher.

Presented to staff and governors:
Review date: September 2022

Our Lady of Lourdes Catholic Primary School
Staff (and Volunteer) Acceptable Usage Agreement

All devices, server and computer systems are owned by the school and are made available to staff to enhance their professional activities, including planning, teaching, research, administration and management.

This Acceptable Use Policy is intended to ensure:
▪ that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
▪ that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
▪ that staff are protected from potential risk in their use of IT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to IT to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Usage Agreement
I understand that I must use school IT systems in a responsible way, to ensure there is no risk to my safety or the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, educate pupils in the safe use of IT and embed Online Safety in my work.

For my professional and personal safety:
▪ I understand the school will monitor my use of IT, email and other digital communications.
▪ I understand the rules set out in this agreement also apply to use of school IT systems outside of school and to the transfer of personal data.
▪ I understand that the school IT systems are primarily intended for educational use.
▪ I will password protect my laptop and any other device.
▪ I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may access it.
▪ I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it and report the incident. I will not use anyone else's password if they reveal it to me.
▪ I will not allow unauthorised individuals to access school or Trust systems.
▪ I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school IT systems:

▪ I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
▪ I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
▪ I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images.
▪ I will follow the school's policy on the use of mobile phones.
▪ I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
▪ I will not engage in any online activity that may compromise my professional responsibilities.
▪ I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Head Teacher.

Social Contact and Social Networking
▪ I understand that communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, web-cams, websites and blogs.
▪ I understand that staff and volunteers should not share any personal information with pupils. They should not request, or respond to, any personal information from the child/young person. If a pupil seeks to establish contact, or if this occurs coincidentally, the adult should exercise his or her professional judgment in reporting the information and should not respond directly, following Child Protection procedures if appropriate.
▪ I understand that staff and volunteers must not give their personal contact details such as phone number; home or personal e-mail address or social networking details to pupils.
▪ I understand that it is recommended that staff ensure that all possible privacy settings are activated to prevent pupils from making contact on personal profiles and to prevent students from accessing photo albums or other personal information which may appear on social networking sites.
▪ I understand that staff must not have any pupils or any ex-pupils under the age of 18 as friends on their social networking sites. Staff are advised not to have any online friendships with any young people under the age of 18, unless they are family members or close family friends. Staff are advised not to have online friendships with parents or carers of pupils, or members of the governing body/trustees, where the basis of this relationship has been through the school. It is acknowledged that especially in our school where it is a key part of the Catholic community, staff may have pre-existing relationships with individuals that later become parents of children in the school. Where such online friendships exist, staff must ensure that appropriate professional boundaries are maintained.
▪ I understand that staff are personally responsible for what they communicate in social media and must bear in mind that what is published might be read by us, pupils, the general public, future employers and friends and family for a long time. Staff must ensure that their on-line profiles are consistent with the professional image expected by us and should not post material which damages the reputation of the school or which causes concern about their suitability to work with children and young people. Those who post material which may be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct which may be dealt with under the school's disciplinary procedure.

Even where it is made clear that the writer's views on such topics do not represent those of the school, such comments are inappropriate.

The school and local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

▪ When I use mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

▪ I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).

▪ I will ensure that my data is regularly backed up.

▪ I will not upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access.

▪ I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

▪ I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed.

▪ I will not disable or cause damage to school equipment or equipment belonging to others.

▪ I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. Therefore USB removable storage devices must not contain personal information about pupils including assessment data or names, unless these are suitably encrypted: the school encourages the use of Google Drive.

▪ I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

▪ I will ensure that I have permission to use the original work of others in my own work.

▪ Where work is protected by copyright, I will not download or distribute copies other than in accordance with the Exceptions to Copyright: Education and Teaching guidance (IPO).

I understand that I am responsible for my actions in and out of the school:

▪ I understand that this Acceptable Use Agreement applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

▪ I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action and in the event of illegal activities, the police will be involved.

I have read and understood the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name
Signed
Date
Please list the make and serial number of any school devices in your possession

Our Lady of Lourdes Catholic Primary School

Online Safety Rules

These Online Safety Rules help to protect pupils in our school by describing acceptable and unacceptable use of IT.

● It is a criminal offence to use a computer or network for a purpose not permitted by the school.
● Irresponsible use may result in the loss of network or Internet access.
● All network and Internet use must be appropriate to education.
● Users must take care not to reveal personal information through any online communication.
● Users must not use their school e-mail to send inappropriate or malicious e-mails.
● Users must not attempt to make contact with staff via social networking sites, e-mail or instant messaging (IM).
● Users must follow all Online Safety rules when using the school's network or Internet.

Stay Safety SMART

Each school may exercise its right to monitor the use of computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place. If the system is used for criminal purposes or for storing unauthorised or unlawful text, images or sound, the police will be called.

Key Stage 1

Think… then click

These rules help us to stay safe on the Internet:

▪ I only use the internet when an adult is with me.
▪ I think before I click on buttons or links.
▪ I can search the Internet with an adult.
▪ I always ask if I get lost on the Internet.
▪ I tell a teacher or trusted adult if I see something I don't like.
▪ I know that online people are really strangers.
▪ I am responsible and never share private information.
▪ I am kind and polite online.

Key Stage 2

Think… then click

Online Safety Rules for KS2:

▪ I ask permission before using the Internet.
▪ I only use websites which are appropriate to my learning.
▪ I am cautious online; I think before I click on buttons or links.
▪ I tell an adult if there is anything I feel uncomfortable with and immediately minimise any website I am unsure about.
▪ I use safe search tools and know I should analyse information for factual accuracy and reliability.
▪ I keep passwords secure and never share personal information.
▪ I communicate politely and respectfully online.

▪ I communicate and collaborate online with people I know and have met in real life, or a trusted adult has approved.
▪ I never arrange to meet anyone I have met online.

Pupil/parent agreement

All pupils use technology, including the Internet, as an essential part of their learning. Pupils and their parents/carers are asked to sign this document to show that the Online Safety rules have been discussed, understood and agreed.

Pupil Agreement
▪ I have read and understood the Online Safety Rules.
▪ I will use the computer, network and Internet in a responsible way at all times.
▪ I know that the network, Internet access and my school e-mail will be monitored.
Name: Class:
Signed: Date:

Parental Consent
I have read and understood the Online Safety rules. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate this is a difficult task. I understand the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

_____

The following services are available to pupils and are hosted by Google as part of G Suite:
▪ Classroom - accessing learning through the cloud
▪ Docs, Sheets and Slides - word processing, spreadsheet and presentation software

Using these and other online tools, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and staff. These services are entirely online and available 24/7 from any Internet-connected device. The school believes that use of these tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account.

Name:
Signed:
Date:

Online Safety: What to do if... guidance

Concern: An inappropriate website is accessed unintentionally by a pupil or member of staff.

1. Play the situation down; don't make it into a drama.
2. Report to the Head Teacher and decide whether to inform parents of any pupils who viewed the site.
3. Inform the IT technician and ensure the site is filtered.

Concern: An inappropriate website is accessed intentionally by a pupil.

1. Refer to the Online Safety rules and agreement signed by the pupil.
2. Report to the Head Teacher.
3. Agree the appropriate sanctions in line with the school's Behaviour Policy.
4. Notify the pupil's parents/carers.
5. Inform the IT technician and ensure the site is filtered (if necessary).

Concern: An inappropriate website is accessed intentionally by a staff member.

1. Ensure all evidence is stored and logged.
2. Report to the Head Teacher.
3. Refer to the Acceptable Use Agreement that was signed by the staff member, and apply the appropriate disciplinary procedures.
4. Inform the IT technician and ensure the site is filtered (if necessary).
5. If the material is of an illegal nature, contact the police and follow their advice.

Concern: An adult uses school IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Head Teacher and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the Head Teacher should then:

▪ Remove the device to a secure place.
▪ Instigate an audit of all IT equipment by the schools IT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
▪ Identify the precise details of the material.
▪ Take the appropriate disciplinary action.
▪ Inform the Chair of Governors and CEO of the incident.

4. In an extreme case where the material is of an illegal nature:

▪ Contact the police and follow their advice.
▪ If requested, remove the device to a secure place and document what you have done.

Concern: An online bullying incident directed at a child, inside or outside of school time.

1. Advise the child not to respond to the message.
2. Report to the Head Teacher.
3. Refer to relevant policies and apply appropriate sanctions.
4. Secure and preserve any evidence through screenshots and printouts.

5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police and/or other agencies if necessary.

Concern: Malicious or threatening comments are posted online about member of the school community (including pupils and staff).
1. Report to the Head Teacher.
2. Secure and preserve any evidence. Consider sending the evidence to CEOP at https://www.ceop.police.uk/Contact-Us/
3. Inform and request the comments be removed if the site is administered externally.
4. Endeavour to trace the origin and ask them to remove the comments.
5. Inform the police and/or other agencies if necessary.

Concern: You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with them.
1. Report to the Head Teacher and/or Designated Safeguarding Lead.
2. Contact the child's parents/carers.
3. Secure and preserve any evidence*.
4. Advise the child on how to terminate the communication.
5. Contact CEOP at https://www.ceop.police.uk/Contact-Us/
6. Inform the police and/or other agencies if necessary.
7. Consider delivering an Online Safety workshop for the school community.
* In cases of sexting, where there are images of children involved, you must confiscate the device and follow the above procedures. Never make or send copies of any images as this in itself is a crime. Further advice is available here.

Concern: You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child.
1. Report to the Head Teacher and/or Designated Safeguarding Lead.
2. Contact the child's parents/carers.
3. Advise the child and parents/carers on appropriate games and content. You may want to use LGfL template letters to inform all or targeted parents.
4. If the game is played within the school environment, ensure that the IT technician blocks access to the game.
5. Consider the involvement of social services.
6. Consider delivering an Online Safety workshop for the school community.

Concern: You are aware of social network posts/pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.
1. Report to the Head Teacher.

2. Contact the poster or page creator and discuss the issues in person, asking them to remove the post(s).
3. Provide staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
4. Consider delivering an Online Safety workshop for the school community.

Online Safety Incident Log

Date of the Incident	Description of the Occurrence (What happened, including details of any information compromised.)	Immediate Corrective Action (What was done to minimise the impact of the incident?)	Further Action Tasks to be undertaken to prevent reoccurrence.	Legal Implications Any legal ramifications e.g. Data Protection Act.	Closed Date To be discussed with and closed by the SIRO/Head Teacher

Password Guidance

Passwords are an important aspect of information security, and are the usual way to protect access to information. As such, all members of staff with access to IT systems are responsible for taking the appropriate steps to select and secure their passwords. These steps include:

▪ Setting up log in passwords and screensaver passwords on laptops and other devices.
▪ Keeping passwords secure from pupils, staff and others, including family members.
▪ Using different passwords for accessing school systems to those used for personal purposes.
▪ Choosing passwords that are difficult to guess, or difficult to obtain by watching staff log in.
▪ Adding numbers or special characters to increase security.
▪ Changing passwords regularly e.g. termly.
▪ Staff should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.
▪ Ensuring that there is a limit on the number of consecutive failed log in attempts.