

Our Lady's RC Primary School



ICT Online Safety Policy

Date Adopted	Spring 2015
Last reviewed by Staff	September 2020
Last reviewed by Governors	September 2020
Person Responsible	Miss G Cunningham
Date of Next Review	Autumn 2021
Version	2.1
Document Reference	2.38

Signed: *Miss G Cunningham* (Online Safety Lead)

Date: 02.9.2020

Signed: *[Signature]* (Headteacher)

Date: 02.9.2020

Signed: *[Signature]* (Chair/Governor)

Date: 02.09.2020

"Learning and loving together; we grow with Jesus"

Our Core Values

During Summer 2020 workshops, we revisited both our Mission Statement and Core Values. This involved everyone in discussion, reflection and prayer about the values, Mission and Aims of our Catholic school. There was a calling to all to re-commit to our purpose and to work together to understand our roles and responsibilities as part of Our Lady's



During the workshops, the feedback from parents, and the views expressed by the children during sessions played a prominent role in the decisions we made.

Our Mission Statement is:

"Learning and loving together; we grow with Jesus"

The Core Values that provide the foundation for that Mission are:

**Faithful
Nurturing
Respectful**

**Positive
Forgiving
Honest**

**Safe
Fair**

NURTURE

The School's six nurturing principles sum up our practice and theory. They underpin the context, organisation and curriculum.

1. Children's learning is understood developmentally
2. The classroom offers a safe base
3. the importance of nurture for the development of wellbeing
4. Language as a vital means of communication
5. All behaviour is communication
6. The importance of transition in children's lives



Our Mission is represented by this design. As with the statement itself, the logo was developed by all stakeholders, with the children in particular providing the symbolic ideas of **growth – the tree**, **love – the hearts** and **Christ – the Cross**

Development / Monitoring / Review of this Policy

This online-safety policy has been developed by a working group made up of: *HT| ICT Coordinator | Staff – including Teachers, Learning Support & ICT technician/ Governors and parents.*

Schedule for Development / Monitoring / Review

The implementation of this online-safety policy will be monitored by the:	<i>Online-Safety / ICT Leader and the SLT</i>
Monitoring will take place at regular intervals:	<i>Half yearly unless deemed appropriate to do so sooner.</i>
The <i>Governing Body</i> will receive a report on the implementation of the online-safety policy generated by the monitoring group (which will include anonymous details of online-safety incidents) at regular intervals:	<i>HT's Report to Gobs and discussion between ICT Lead and Governor responsible for ICT</i>
The online -safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online-safety or incidents that have taken place. The next anticipated review date will be:	<i>See front cover</i>
Should serious online-safety incidents take place, the following external persons / agencies should be informed:	<i>LA Safeguarding Officer, CEOP, IWF & Police</i>

The school will monitor the impact of the policy using the logs of reported incidents, monitoring logs, surveys and questionnaires of a wide group including pupils.

Scope of the Policy

This policy applies to all members of Our Lady's RC Primary (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers HTs 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Our Lady's RC Primary will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online -safety behaviour that take place out of school.

Educating Children on E Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online-safety is therefore an essential part of the school's online-safety provision. Children and young people need the help and support of the school to recognise and avoid online-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The online-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online-safety curriculum will be provided as part of the Computing / PSCHÉ / other lessons and will be regularly revisited
- Key online-safety messages will be reinforced as part of a planned programme of assemblies
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff must act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.

Educating Parents / Carers on Online Safety

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. We will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, School Blog
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

Educating Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online -safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online-safety as a training need within the appraisal process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The Online -Safety Coordinator will receive regular updates through attendance at external training events (e.g. from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online-Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings
- The Online-Safety Coordinator will provide advice / guidance / training to individuals as required.

Educating Governors

Governors will take part in online -safety training / awareness sessions, with particular importance for those who are members of the Resources Committee. This may be offered in a number of ways:

- Attendance at training provided by the LA or other relevant organisation
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will also need to ensure that the relevant people will be effective in carrying out their e-safety responsibilities:

- The school will work in partnership with Wigan Council to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online-Safety Lead or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Monitoring software called Securus is used to monitor usage of the school curriculum computers and network. Securus captures records of misuse and unacceptable behaviour, such as swearing, accessing inappropriate or filtered websites and explicit images and identifies the user involved. Securus covers all internet use, all software, teachers' laptops, all websites, email, use of chat, forums and other social networking sites. All inappropriate use, misuse or abuse is reviewed by senior staff, who then decide on the action to be taken.
- The school curriculum network is filtered through the Wigan Council filtering system.
- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school /technical systems and devices.
- All users will be provided with a username and password by (ICT Technician) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- Internet access is filtered for all users. There is a clear process in place to deal with requests for filtering changes.
- The ICT technician will regularly monitor the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device

- The school has a set of clear expectations and responsibilities for all users bring their own devices into school
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated

- Where possible devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device must be reported
- Any user leaving the school will follow the policy principles

Use of digital and video images – see policy statement

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This is covered within the agreement with parents when a child joins the school.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed

- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils / pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with a school email addresses for educational use.
- Pupils should be taught about online-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

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:

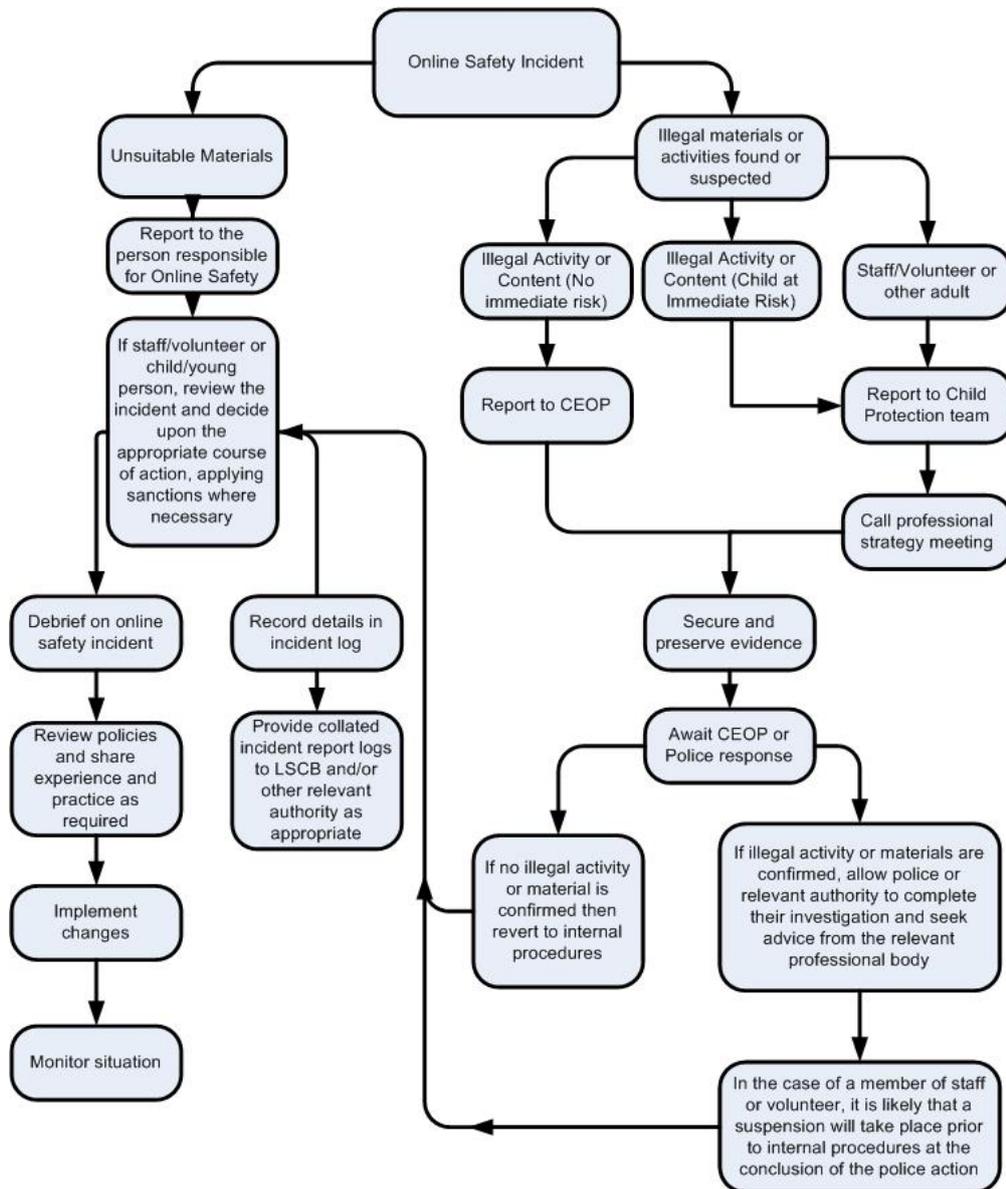
	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978		X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.		X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008		X
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986		X
Pornography	X	
Promotion of any kind of discrimination	X	
Threatening behaviour, including promotion of physical violence or mental harm	X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	X	
Using school systems to run a private business	X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy	X	
Infringing copyright	X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)	X	
Creating or propagating computer viruses or other harmful files	X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)	X	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the

machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.