St. Jerome's Catholic Primary School

Online Safety and Acceptable Use Policy

The review and maintenance of this policy is the responsibility of the Full Governing Body.

Aim: The aim of this policy is to set out the ways in which the school will:

- educate all members of the school community about their rights and responsibilities with the use of technology;

- build both an infrastructure and culture of e-Safety;

- work to empower the school community to use technology including the Internet as an essential tool for life-long learning.

Status: Statutory

Purpose:
- To put into place effective management systems and arrangements which maximise the educational and social benefit of exploiting the opportunities of using ICT whilst minimising any associated risks.

- To describe actions that should be put into place to redress any concerns about welfare and safety as well as how to project the children, young people and staff of St. Jerome's Catholic Primary School from risks and infringements.

Relationship to other policies:

This Online Safety Policy is used in conjunction with other school policies, in particular the Child Protection & Safeguarding, Anti-Bullying and Behaviour Policies, those policies relating to particular aspects of Online Safety, Online Safety Acceptable Use Policies (AUPs) and the Data Protection Policy.

Scope of Policy

This policy applies to all members of the school community (including staff, governors, children, technicians, volunteers, parents / carers, visitors and community users) who have access to and are users of school ICT systems.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage Online Safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate Online Safety behaviour that take place in and out of school.

The Online Safety Policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to Online Safety or incidents that have taken place.

Roles and responsibilities

The Headteacher (Mrs K Monaghan) is responsible for ensuring the safety (including Online Safety) of all members of the school community, though the day-to-day responsibility for e-Safety can be delegated.
An Online Safety Leader (Mrs Beckingham) is appointed to work with the Designated Safeguarding Leaders (Mrs K Monaghan, Mrs D. Hall) who will have an overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

An Online Safety working group works with the Online Safety Leader to implement and monitor the Online Safety Policy and Acceptable Use Policies (AUPs). This group is made up of the Online Safety Leader, Head teacher who also fulfils the role of Designated Safeguarding Lead, teacher responsible for the School Council, Safeguarding Governor, member of support staff and children. Children are part of this group, working with them through the School Council, to contribute their knowledge and use of technology.

Role	Responsibility
Governors	• Approve and review the effectiveness of the Online Safety Policy • Delegate a governor to act as Online Safety link • Online Safety Governor works with the Online Safety Leader to carry out regular monitoring and report to Governors
Headteacher and Senior Leaders	•Ensure that all staff receive suitable CPD to carry out their Online Safety roles • Create a culture where staff and learners feel able to report incidents • Ensure that there is a system in place for monitoring Online Safety • Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or children • Inform the Local Authority (LA) about any serious Online Safety issues • Ensure that the school infrastructure / network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review Online Safety with the school's technical support Online Safety Leader
Online - Safety Leader	• Monitor concerns logged by staff and inform others of Online Safety incidents, including the Online Safety Governor • Lead the establishment to review Online Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to Online Safety • Organise training and advice for staff • Attend updates and liaise with the LA Online Safety staff and technical staff • Meet with the Designated Safeguarding Lead to regularly discuss Online Safety incidents and developments • Lead and monitor a progressive Online Safety curriculum for pupils
Teaching and Support Staff	Participate in any training and awareness raising sessions • Read, understand and sign the Staff AUP • Act in accordance with the Staff AUP and Online Safety Policy • Complete the school's 'Cause for Concern Form' to report any suspected misuse or problems to the Online Safety Leader and file copies within the Online Safety Concerns File and the child's Class Concerns File. • Follow Child Protection procedures for all serious concerns • Monitor technology use in lessons, extracurricular and extended school activities • Plan appropriate Online Safety learning opportunities as part of a progressive Online safety curriculum • Respond to opportunities to model and discuss Online safety

Children	• Read, understand and sign the Child AUP and the agreed class Internet rules • Participate in Online Safety activities, follow the AUP and report any suspected misuse • Understand that following the AUP and class Internet rules protects them out of school, including time spent on electronic devices • Support their friends to use the internet responsibly and safely
Parents and Carers	• Endorse (by signature) the Child AUP • Discuss Online Safety issues with their child(ren) and monitor their home use of technology devices (including mobile phones and games devices) and the Internet • Access the school website in accordance with the relevant school AUP • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any Online Safety concerns that relate to the school
Technical Support Provider	•Ensure the school's ICT infrastructure is as secure as possible • Ensure users may only access the school network through an enforced password protection policy for those who access children's data • Maintain and inform the Senior Management Team of issues relating to filtering • Keep up to date with Online Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be monitored • Be reported to the Online Safety Leader for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign the Technician AUP detailing their extra responsibilities

Education of children

A progressive planned Online Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

• Key messages are reinforced through an assembly and a discrete Online Safety lesson each term, along with Safer Internet Week (February), anti-bullying week (November) and throughout all lessons where appropriate.

• Children are reminded of key Online Safety messages frequently even when they have already been taught them in previous years.

• Children are taught to keep themselves safe online and to be responsible in their use of different technologies.

• Children are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage children to use specific search terms to reduce the likelihood of coming across unsuitable material.

•In lessons where Internet use is pre-planned, children are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches. Staff use the agreed search engines.

• Children are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.

•Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

• Children will review class rules and sign this as their annual AUP at the beginning of each

school year, which will be shared with parents and carers.

• Children are taught how to use the internet before they go on it.

• Children are taught how computers work to increase their understanding of how it can be used to keep them safe and the possible dangers.

• The internet will be used for educational purposes.

Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school.

They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents and carers to do this by:

• Providing clear AUP guidance which they are asked to sign with their children when they first join the school and regular termly class newsletters and website updates;

• Raising awareness through activities planned by children;

• Inviting parents to attend activities such as Online Safety week, Online Safety assemblies or other meetings as appropriate.

Training of Staff and Governors

There is a planned programme of Online Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs.
This includes:
• An annual audit of the Online Safety training needs of all staff.

• All staff receiving annual Online safety training (Hays Online Training)

• All new staff receiving Online Safety training as part of their induction programme.

•The Online Safety Leader receiving regular updates through communication with LA, training sessions and by reviewing regular newsletters from Think U know CEOP.

• This Online Safety Policy and its updates being shared and discussed in staff meetings.

• The Online Safety Leader providing guidance and training as required to individuals and seeking LA support on issues.

• Staff and governors are made aware of the UK Safer Internet Centre helpline **0844 3814772**.

• Opportunities will be planned for the children to teach the adults what they know about the developments of technology.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Anti-Bullying and Behaviour Policies.

• The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

• All incidents of cyberbullying reported to the school will be recorded on a school 'Cause for Concern' Form.

• The school will follow procedures to investigate incidents or allegations of cyberbullying.

• Children, staff and parents and carers will be advised to keep a record of the bullying as evidence.

• The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses and contacting the service provider and the police.

• Children, staff, parents and carers will be required to work with the school to support the approach to cyberbullying and the school's Online Safety ethos.

• Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:

o The bully being asked to remove any material deemed to be inappropriate or a service provider being contacted to remove content if the bully refuses or is unable to delete the content.

o Internet access being suspended at the school for a period of time after the child has received a warning. The period of time is dependent on how serious the incident is. Other sanctions for children and staff also being used in accordance to the school's AntiBullying Policy, Behaviour Policy or AUP.

o Parent and carers of the child being informed.

o The police being contacted if a criminal offence is suspected.

Technical Infrastructure

The person responsible for the school's technical support will sign the Staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

• The School ICT systems are managed in ways that ensure that the school meets Online Safety technical requirements

• There are regular reviews and audits of the safety and security of school ICT systems.

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc. from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

o the downloading of executable files by users

o the extent of personal use that users (staff / children / community users) and their family members are allowed on laptops and other portable devices used out of school

o the installation of programs on school devices unless permission is given by the technical support provider or Computing Leader

o the use of removable media (e.g. memory sticks) by users on school devices (see Personal Data Policy for further detail)

o the installation of up to date virus software

• Access to the school network and Internet will be controlled with regard to:

o users having clearly defined access rights to school ICT systems through group policies

o adult users being provided with a username and password

o children being provided with a username (Early Years Foundation Stage provided with a class username)

o users being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log in details

o users must immediately report any suspicion or evidence that there has been a breach of security

o an agreed process being in place for the provision of temporary access for supply and trainee teachers onto the school system. Regular supply teachers must sign the Staff AUP and are made aware of this Online Safety Policy. Occasional visitors are to sign the Visitor AUP.

o Key Stage 1 children's access to the Internet will be by adult demonstration with direct supervised access to specific and approved online materials

o Key Stage 2 children will be trusted to access the Internet appropriately but regular check-ups will be made. Children will use age-appropriate search engines and online tools and activities, which will be adult directed

• The Internet feed will be controlled with regard to:

o the school maintaining a managed filtering service provided by an educational provider

o the school monitoring Internet use

o requests from staff for sites to be removed from the filtered list being approved by the Senior Management Team

o any filtering issues being reported immediately to the Schools Broadband helpline.

• The ICT System of the school will be monitored with regard to:

- the school ICT technical support regularly monitoring and recording the activity of users on the school ICT systems

- Online Safety incidents being documented and where appropriate reported immediately to the Online Safety Leader who will arrange for these to be dealt with immediately in accordance with the AUP.

Data Protection

The School's General Data Protection Policy provides full details of the requirements that need to be met in relation to GDPR 2018.

The school will:
• 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

• ensure that users are properly "logged-off" at the end of any session in which they are accessing personal data and "lock" computers when away from the computer

• store or transfer data encryption and secure password protected devices

• make sure data is deleted from the device once it has been transferred or its use is complete.

Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers and to provide information about the school on the website.

The school will:

• When using digital images, instruct staff to educate children about the risks associated with the taking, use, sharing, publication and distribution of images including their publication on social networking sites.

• Allow staff to take images to support educational aims, but follow guidance in the Acceptable Use Policy (AUP) concerning the sharing, distribution and publication of those images.

• Make sure that images or videos that include children will be selected carefully and will not provide material that could be reused.

• Make sure that children's full names will not be used anywhere on the school website, particularly in association with photographs.

• Written permission from parents or carers will be obtained before images or videos of children are electronically published.

• Keep the written consent where children's images are used for publicity purposes, until the image is no longer in use.
• Publish a policy regarding the use of photographic images of children, which outlines policies and procedures.

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The school will:

-with respect to email

- Ensure that all school business will use the official school email service.

o Ensure that any digital communication between staff and parents and carers is professional in tone and content and through a school email address.

o Make users aware that email communications may be monitored.

o Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

o Teach children about email safety issues through the scheme of work and implementation of the AUP.

o Ensure that personal information is not sent via email.

o Only publish official class email address specific for homework not for contact

-with respect to social media

o Only use social media and social networking sites where it is appropriate for educational purposes and with permission of the Headteacher.

o Provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure the site is age appropriate.

o Make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Senior Management Team.

o Inform staff not to run social network spaces for children

- with respect to personal publishing

o Teach children via age appropriate sites that are suitable for educational purposes. The school will moderate them.

o Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

o Register concerns regarding children's use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning children's underage use of sites.

o Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction.

o Outline safe and professional behaviour

- **with respect to mobile phones**

o Allow staff to bring mobile phones into school but inform them that they must only use mobile phones during break, lunchtimes or during non-contact when they are not in contact with children unless they have the permission of the Headteacher. These must be turned off or onto silent during the school day. They are not allowed to take photographs or videos in school for any purpose without the express permission of the Senior Management Team.

o Advise staff not to use their personal mobile phone to contact children, parents and carers. Use for school trips is an exception but the Headteacher will be informed of their use.

o Children are only allowed to bring mobile phones into school in exceptional circumstances with the permission of the Headteacher.

The following table shows how the school considers how all these methods of communication should be used.

	Staff & Other Adults				Children			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/presence	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on personal mobile phones/devices				x				x
Taking photos on school devices (parental permission obtained)	x						x	
Use of personal email addresses in school, or on the school network				x				x
Use of school email for personal emails				x				x
Use of chat rooms/facilities				x				x
Use of text messaging		x						x
Use of social networking sites such as Facebook				x				x
Educational websites with an element of social networking (being able to communicate with others)		x				x		
Use of blogs			x				x	
Use of Twitter			x					x
Use of YouTube (school account)	x						x	
Use of Skype			x				x	

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the Online Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology

- considering whether the technology has access to inappropriate material.

However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use. Children will be educated about dealing with the risks.

All users will be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to incidents

The school will follow Sefton's flowcharts to respond to illegal and inappropriate incidents as listed in those publications.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

- Staff will record all concerns and actions taken on 'Cause for Concern' Forms which will be monitored by the Online Safety Leader in the School Online Safety incident file and in the class concerns files.

- The Designated Safeguarding Leaders will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.

- The school will manage Online Safety incidents in accordance with the School Behaviour Policy where appropriate.

- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.

- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Sefton Local Safeguarding Children Board (LSCB) and escalate the concern to the police.

- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser, Local Authority Designated Officer (LADO) or Senior ICT Adviser.

Sefton Safeguarding Advisor Information
Local Area Designated Officer SafeGuarding and Child Protection 01519343783

The police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images

- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation

- adult material that potentially breaches the Obscene Publications Act in the UK

- criminally racist material

Sanctions and Disciplinary proceedings Sanctions and disciplinary procedures will be taken where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

• pornography, adult or mature content

• promotion of any kind of discrimination, racial or religious hatred

• personal gambling or betting

• personal use of auction sites

• any site engaging in or encouraging illegal activity

• threatening behaviour, including promotion of physical violence or mental harm

•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

• using school systems to run a private business

• use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Schools Broadband and the school

• uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions

• revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)

• creating or propagating computer viruses or other harmful files

• carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet:

In addition the following indicates school policy on these uses of the internet:

	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Online gaming (educational)	x		
Online gaming (non-educational)			x
Online gambling			x
Online shopping/commerce		x	x
File sharing (using peer to peer networks) but not for files containing personal data)	x		

Sanctions for misuse: Children

Appropriate possible sanctions are detailed in the grid below. Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore marks may appear in more than one column. The marks in place are actions, which must be followed.

Incidents	Refer to class teacher	Refer to key stage leader	Refer to head teacher	Refer to police	Refer to technical support staff for action re filtering etc.	Inform parents/carers	Removal of network/ internet access rights	Warning	Further action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			x	x		x			
Unauthorised use of non-educational sites during lessons		x					x	x	
Unauthorised use of mobile phone / digital camera / other handheld device			x						
Unauthorised use of social networking / instant messaging / personal email			x						
Unauthorised downloading or uploading of files		x			x		x		
Attempting to access or accessing the school network, using another children's account	x					x		x	
Attempting to access or accessing the school net work, using the account of a member of staff.			x				x		
Corrupting or destroying the data of other users			x			x	x		x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.			x			x	x		x
Continued infringements of the above, following previous warnings or sanctions			x			x	x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x			x	x	x	
Using proxy sites or other means to subvert the school's filtering system			x		x	x	x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident			x		x	x			
Deliberately accessing offensive or pornographic material and failing to report the incident			x		x	x	x	x	x
Receipt or transmission of material the infringes the copyright of another person or infringes the data protection act	x					x		x	

Sanctions/ Actions Staff

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore marks may appear in more than one column. The marks in place are actions, which must be followed.

Incidents	Refer to key stage leader	Refer to head teacher	Refer to local authority /HR	Refer to LADO/ Police	Refer to technical support staff for action re filtering etc.	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x		L, P	x			x
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email	x	x				x		
Unauthorised downloading or uploading of files	x	x				x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x				x		
Careless use of personal data e.g. holding or transferring data in an insecure manner		x				x		
Deliberate actions to breach data protection or network security rules		x						x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x						x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to other staff		x				x	x	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners		x		L				
Breach of the school e –safety policies in relation to communication with learners		x		L				
Using personal email/ social networking/instant messaging/text messaging to carry out digital communication with children		x		L				
Actions which could compromise the staff members professional standing		x				x		
Actions which could bring the school into disrepute or breach the integrity or ethos of the school		x				x		
Using proxy sites or other means to subvert the school's filtering system		x			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident		x		L	x	x		
Deliberately accessing offensive or pornographic material and failing to report the incident		x		L	x			x
Breaching copyright or licencing regulations		x				x		
Continued infringements of the above, following previous warnings or sanctions		x					x	x

Policy date: September 2021

Review date: September 2022