St Luke's RC Primary School

Online Safety Policy
June 2020

"At St. Luke's School we follow the example of Christ. By being God's disciples here on Earth. We strive to be the best that we can be. To do the best that we can do and to make God proud."

1 – To be ratified by Governors in Autumn 2020

Policy Number	1
Target Audience	All stakeholders
Approving Committee	FGB
Last Review Date	June 2020
Next Review Date	July 2021
Policy Author	C. Barrett

Version Control			
Version No	**Date Approved**	**Reviewed By**	**Changes**
V1	June 2020	C.Barrett	New policy

Contents

Introduction

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

Governors:

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:
The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community.

- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- The Headteacher and another member of the Senior Leadership Team have access to the RM Smoothwall which combines a powerful reporting suite, real-time activity monitoring, social media controls and bandwidth optimisation, so they can see and control everything school users do on the web – even when they're using their own devices on your network, or taking your devices on the road.

Online Safety Coordinator:
Our Computing coordinator is responsible for ensuring:

- Leads the Online Safety committee and/or cross-school initiative on Online Safety
- Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provides training and advice for staff
- Receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- Reports regularly to Senior Leadership Team

Managed Service Provider, RM:
Our Managed Service Provider, RM is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the Online Safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy

Teaching and Support Staff
Are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)

- They report any suspected misuse or problem to the Online Safety Co-ordinator and the Headteacher for investigation/action

Designated Person for Child Protection
Should be trained in Online Safety issues and be aware of the potential for serious child Protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate Online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils

- Using the school ICT systems and mobile technologies in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. At KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers
The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local Online Safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student/Pupil Acceptable Use Policy
- Accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

Community Users
Community Users who access school ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

Online Safety Education and Training

Education – Pupils

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of Computing and PSHE and will be regularly revisited – this will cover both the use of computing and new technologies in and outside school

- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and lesson activities
- Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

Education & Training – Staff

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

- A planned programme of formal Online Safety training will be made available to staff. 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 performance management process.
- All new staff will receive a copy of the Online Safety policy as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies

Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				Students/Pupils			
Communication method or device	Allowed	Allowed at certain times and places	Allowed for selected staff and at certain times	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	☑	⚠	⚠	☒	☑	⚠	⚠	☒
Mobile phones may be brought to school		⚠						☒
Use of mobile phones in lessons				☒				☒
Use of mobile phones in social time		⚠						☒
Taking photos on personal mobile phones or other camera devices				☒				☒
Use of personal hand held devices e.g. PDAs, PSPs		⚠						☒
Use of personal email addresses in school, or on school network	☑							☒
Use of school email for personal emails			⚠					☒
Use of chat rooms / facilities				☒				☒
Use of instant messaging				☒				☒
Use of social networking sites				☒				☒
Use of blogs	☑						⚠	

 This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Students/Pupils**
Mobile phones may be brought to school	Can be used when children are not around and in areas where	
Use of mobile phones in social time	During breaks and before/after school	
Use of personal hand held devices e.g. PDAs, PSPs	During breaks and before/after school	
Use of personal email addresses in school, or on school network	Not to be used for school purposes	
Use of school email for personal emails	Before/after school and during breaks	

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 certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions	☑	⚠	⚠	☒	☒
child sexual abuse images					☒
promotion or conduct of illegal acts, e.g. 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 in UK					☒
pornography					☒
promotion of any kind of discrimination					☒
promotion of racial or religious hatred					☒
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 SCC and / or 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 / personal information, databases, computer / network access codes and passwords)				☒	
Creating or propagating computer viruses or other harmful files				☒	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☒	
Online gaming (educational)				☒	
Online gaming (non educational)				☒	
Online gambling				☒	
Online shopping / commerce					
File sharing					☒
Use of social networking sites				☒	
Use of video broadcasting e.g. YouTube				☒	
Accessing the internet for personal or social use (e.g. online shopping)					
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses				☒	

Good practice guidelines

Email

Best practice

☑ **DO**

Staff, supply staff and pupils should only use their school email account to communication with each other

Safe practice

Check the school Online Safety policy regarding use of your school email or the internet for personal use e.g. shopping

Poor practice

☒ **DO NOT**

Staff: don't use your personal email account to communicate with students/pupils and their families, in accordance with the Online Safety policy.

Images, photos and videos

Best practice

☑ **DO**

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Poor practice

☒ **DO NOT**

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the Online Safety policy.

Don't retain, copy or distribute images for your personal use.

Internet

Best practice

☑ **DO**

Understand how to search safely online and how to report inappropriate content.

Safe practice

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

☒ **DO NOT**

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the Online Safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones

Best practice

☑ **DO**

Staff: If you need to use a mobile phone while on school business (trips etc), the school will should provide equipment for you.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Only use mobile phones for personal use during breaks or after school.

Safe practice

Check the Online Safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

☒ DO NOT

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.

Don't retain service student/pupil/parental contact details for your personal use.

Social networking for Staff (e.g. Facebook/ Twitter/Instagram)

☑ **DO**

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

Safe practice

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

☒ DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.
Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

Webcams

Best practice

☑ **DO**

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

Check the Online Safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Poor practice

DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the Online Safety policy.

Don't retain, copy or distribute images for your personal use.

Incident Management

Incidents (students/pupils):	Refer to class teacher	Refer to E Safety Coordinator	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention , suspension, exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of mobile phone/digital camera / other handheld device	✓	✓	✓			✓		✓	✓
Unauthorised use of social networking/ instant messaging/personal email	✓	✓	✓		✓	✓	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓		✓	✓	✓	✓	✓
Allowing others to access school network by sharing username and passwords	✓	✓	✓		✓	✓	✓	✓	✓
Attempting to access or accessing the school network, using another student's/pupil's account	✓	✓	✓		✓	✓	✓	✓	✓
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓			✓		✓	✓
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓	✓	✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓	✓	✓	✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓	✓	✓	✓	✓	✓	✓

Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓		✓	
Deliberately accessing or trying to access offensive or pornography	✓	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓	✓	✓	✓	✓	✓	✓

Incidents (staff and community users):	Refer to E Safety Coordinator	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction- reporting to governors, suspension, dismissal
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	✓	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓		✓	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓	✓	✓	✓	✓
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	✓	✓		✓	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓		✓		✓	✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓	✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓	✓	✓	✓
Using personal email / social networking / instant messaging / text	✓	✓	✓	✓	✓	✓	✓

messaging to carrying out digital communications with students / pupils							
Actions which could compromise the staff member's professional standing	✓	✓			✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓			✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓		✓		✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓				✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓	✓

Further information and support

For a glossary of terms used in this document:

http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf

For Online Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:

http://www.salford.gov.uk/d/Online Safety-Practice-Guidance.pdf

R u cyber safe?

Online Safety tips about how to stay safe online:

http://www.salford.gov.uk/rucybersafe.htm

EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**