Policy Reference: 24

E-SAFETY POLICY

Version: 3

Name and Designation of Policy Author(s)	Nina Chwastek, Headteacher	Is this a Statutory Document	No
Approved By (Committee / Group)	Curriculum Committee		
Date Approved	October 2021		
Date Ratified by FGB	n/a		
Date Published	12th October 2021	*Is this to be published publicly on the school website?*	Yes
Review Date	Autumn Term 2024		
Target Audience	Pupils, Staff, Parents and Governors		
Links to Other Strategies, Policies, Procedures, etc.	Anti-Bullying Policy, Personal Social and Health Education Policy, Safeguarding Policy, Behaviour Policy, Social Networking Policy, Acceptable Use of IT Policy.		

Version History

Date	Ver	Author Name and Designation	Summary of Main Changes
Jan 2016	1	Nina Chwastek, Headteacher	Old E-Learning policy updated and put into new standard format
February 2020	2	Nina Chwastek, Headteacher	Updated to take account of new requirement in order to comply with 360Safe Award
September 2021	3	Jessica Quiligotti, Deputy Headteacher	Annual review

Monitoring Compliance with the Policy

Describe Key Performance Indicators (KPIs)	Target	How will the KPI be Monitored?	Which Committee will Monitor this KPI?	Frequency of Review	Lead
Training logs for staff and volunteers are kept up to date	100%	Monitoring of Training Logs	Curriculum	Annually	E-Safety Governor
All staff, volunteers, pupils and governors with access to school email and/or internet have signed the	100%	Review of Acceptable Use Documentation	Curriculum	Annually	E-Safety Governor

appropriate agreement forms					

Contents:

1. Mission Statement
2. Introduction
3. Scope
4. Ethos
5. Objectives
6. Roles and Responsibilities
7. Internet Access
8. Filtering
9. Managing E-Mail
10. Manging Website Content
11. Social Networking and Chat Rooms
12. Mobile Phones
13. Photographic, Video and Audio Technology
14. Assessing Risks
15. Introducing the Policy to Children
16. Maintaining ICT Security
17. Dealing with Complaints and Concerns

Appendix 1: Acceptable Use Agreement: Rules for children using ICT in school
Appendix 2: Acceptable Use Policy: Staff, Governors and Visitors Agreement Form
Appendix 3: Safeguarding Concern Form

1. Mission Statement

Our school community is rooted in the Gospel and the vision of St. Catherine of Siena.

This inspires each of us *'To be who God wants us to be and so set the world on fire.'*

- We are called to love one another as we seek to be the best in all that we learn and do.
- We celebrate and nurture the gifts, talents and skills of everyone.
- We commit ourselves to grow together in faith, love and service.

2. Introduction

This policy has been developed to ensure that all adults in St. Catherine's R.C. Primary School work together to safeguard and promote the welfare of children and young people.

The term E-Safety when used in this policy is used to refer to all fixed and mobile technologies that children may encounter, now and in the future, which allow them to access to content and communications that could raise e-safety issues or pose risk to their wellbeing and safety.

E-Safety is a safeguarding issue not a Computing or ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

The purpose of internet use in school is to help raise educational standards, promote pupil achievement and support the professional work of staff as well as enhance the school's management information and business administration systems.

The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

The internet is part of the statutory curriculum and a necessary tool for staff and children and benefits education by allowing access to worldwide educational resources including aft galleries and museums as well as enabling access to specialists in many fields.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

3. Scope

This policy applies to all staff, volunteers, parents and carers and pupils in the school community of St Catherine's RC Primary School who have access to and are users of school ICT systems both in and out of school. This policy also applies to incidents of cyber-bullying or other e-safety incidents which may take place out of school but are linked to membership of the school.

4. Ethos

It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

All staff have a responsibility to support E-Safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach E-safety protocols.

E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behaviour Policy.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

5. Objectives

- Digital images of children will not be used without the consent of the child's parent or carer.
- Digital images will be stored on the school secure server for use within school, limited by parental consent.
- Anyone accessing school email or school internet has signed an agreement form, or their parents or carers have if they are in Key Stage 1.

6. Roles and Responsibilities

The Headteacher has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

The Headteacher of St. Catherine's R.C. School will ensure that:

- The E-Safety Policy is implemented and compliance with the policy is monitored.
- All staff are included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- The Computing Leader is the lead member of staff for E-Safety and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- The virus protection is regularly reviewed and updated.
- Files are checked regularly on the school's network.
- ICT security is maintained.

The Governing Body of the school will ensure that:

- The Computing Leader reports to the Headteacher and the E-Safety Governor receives information relating to any E-Safety incidents that take place in school
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.

The Computing Leader as the lead member of Staff for E-Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security and liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Ensure all staff and volunteers have access to appropriate ICT training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received a copy of the school's Acceptable Use of ICT Resources document.
- Has a lead role in establishing and reviewing the school E-Safety Policy and documentation.

- Ensure that all staff and volunteers understand and aware of the school's E-Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network for any irregularities

All staff and volunteers have a responsibility to support e-safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

7. Internet Access

Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

The school will maintain a current record of all staff, pupils, volunteers (including PTA members) and governors who are allowed access to the school's ICT systems. The school will maintain a record of pupils whose parents and carers have specifically requested that their child be denied internet access.

<u>Pupils</u>

1. Parents or carers will sign, on behalf of their children, the school's Acceptable Use Agreement (Appendix 1) as part of the Admissions procedure in Foundation Stage and Key Stage 1.
2. Key Stage 2 pupils will read and sign the school's Acceptable Use Agreement. (Appendix 1)
3. Pupils will be taught what internet use is acceptable and what is not and they will be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned appropriately for the pupil's age and maturity.
4. Internet use will be planned to enrich and extend learning activities and reflect the curriculum requirements of the children.
5. Pupils will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be encouraged to question the validity and origins of the information.
6. Pupils will also be taught that copying material is worth little without selectively evaluating the material.
7. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet sourced material in their own work.
8. Pupils will be taught what to do if they experience material that they find upsetting, distasteful or threatening.

9. Pupils will be informed that internet use will be closely monitored and that any misuse or incidents of cyberbullying will be dealt with in accordance with the school's Anti-Bullying Policy and Behaviour Policy.

Staff

1. All staff will sign the school's Acceptable Use Agreement. (Appendix 2)
2. If staff discover an unsuitable site, the URL (address) and content must be reported to the Computing Leader and Headteacher.
3. Staff must ensure that any content they use complies with copyright law.
4. Work logins or passwords must be kept private and secure.
5. Staff will log any incidents of cyberbullying or internet misuse on CPOMS to alert the Headteacher and Designated Safeguarding Leads to such incidents. The Computing Leader will also be made aware, by those detailed above, as necessary.
6. Staff may use the school's photographic or video technology to capture or support educational visits and appropriate curriculum activities.
7. Staff must be aware that the school internet must only be used for school business.
8. Staff will supervise pupils when accessing the internet in school.

All Users

1. All users, including any staff not directly employed by the school, volunteers and governors must read and sign the school's 'Acceptable Use of IT Agreement Form' before being allowed internet access from the school site.
2. All users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain inappropriate images.
3. All users shall not promote any kind of discrimination, racial or religious hatred, threatening behaviour or any other information which may be offensive to colleagues or breaches the integrity of the ethos of St Catherine's RC Primary school or brings the school into disrepute.

ICT Technical Support Provider

The school's ICT technical support provider will be responsible for ensuring that:

1. The school's ICT infrastructure is secure and not open to misuse or malicious attack
2. Users may only access the school's network through a properly enforced password protection policy.
3. Any shortcomings in the infrastructure are reported to the Computing Leader or Headteacher so that appropriate action may be taken.

8. Filtering

The school will work in partnership with parents and carers, the Local Authority, the DfE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing Leader.

Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk).

Regular checks by the Computing Leader will ensure that the filtering methods selected are appropriate, effective and reasonable.

Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

9. Managing E-Mail

Personal e-mail or messaging between staff and pupils should not take place.

Staff must use a school e-mail address if they need to communicate with pupils, parents or carers.

School emails must include this footer:
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

If emails contain confidential or sensitive information or information which identifies an individual these need to be sent securely i.e. password protected or via the egress portal.

Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole class or group e-mail addresses should be used at KS1 and below.

Through the curriculum, pupils are educated about e-safety and the dangers of revealing details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and that they must not arrange meetings with anyone.

Access in school to external personal e-mail accounts may be blocked.

E-mail should be authorised before sending to an external organisation just as a letter written on school headed note-paper would be.

The forwarding of chain letters is not permitted.

Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

10. Managing Website Content

Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

Photographs of pupils will not be used without the written consent of the pupil's parents or carers.

The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.

The Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

The website will comply with the school's guidelines for publications and parents and carers will be informed of the school policy on image taking and publishing, i.e. that images will only be used with parental consent. This is sought upon entry to school.

Use of site photographs will be carefully selected so that any pupils cannot be identified or their image misused, i.e. full names will not be used alongside photographs.

Work will only be used on the website with the permission of the pupil and their parents or carers.

The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Pupils will be taught to consider the thoughts and feelings of others when publishing material on websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate action will be taken.

11. Social Networking and Chat Rooms

Pupils will not access social networking sites in school e.g. 'My Space', 'Facebook', 'Twitter', 'Instagram' or 'Snapchat' or 'Tik Tok'.

Pupils will be taught the importance of personal safety when using social networking sites and chat rooms outside school.

Pupils will not be allowed to access public or unregulated chat rooms.

Newsgroups will be blocked unless an educational need can be demonstrated.

Staff will not exchange social networking addresses or use social networking sites to communicate with pupils. The exception to this is an official St. Catherine's School

social network site, in which case all content will be monitored a designated member of staff.

Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a senior manager should always be sought first and language should always be appropriate and professional.

12. Mobile Phones

Mobile phones will not be used during lessons or formal times in school. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policies.

Use of cameras or video cameras on mobile phones or other personal devices is strictly not allowed by staff, volunteers, governors or pupils.

Staff will be issued with a school mobile phone where contact with pupils or parents and carers is necessary or where mobile phones are used to photograph school activities involving pupils.

Pupils who bring mobile phones (or any other mobile device with internet access) into school in Year 6 must hand them in to the class teacher/phase leader at the start of the day and only collect them at the end of the school day. No other children should bring mobile phones into school unless this has been authorised by a member of the senior leadership team. Phones should then remain with the school office or class teacher/phase leader.

The mobile phone (or similar device) must remain switched off while on school premises.

13. Photographic, Video and Audio Technology

Staff may use school photographic or video technology to capture to support educational visits and appropriate curriculum activities.

Pupils must have permission from a member of staff before making a video or audio recording in school or on educational activities.

Webcam use in school will be appropriately supervised for the pupil's age.

14. Assessing Risks

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material.

However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

15. Introducing the Policy to Children

Responsible Internet use, covering both school and home use, will be taught as part of the Computing curriculum. Each unit of study will include an e-safety element.

Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks of any lesson using the Internet.

Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

16. Maintaining ICT Security

Personal data sent over the network will be encrypted or otherwise secured.

Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

The ICT Technical Support Provider will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

17. Dealing with Complaints and Concerns

Complaints are dealt with through the Complaints Policy. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures.

Appendix 1:

St Catherine's RC Primary School

Acceptable Use Agreement: Rules for children using ICT in school

Use of School Computers

I will:

- Always follow my teacher's instructions.
- Use the computers for school work and homework only.
- Only access the computers using user names and passwords given to me by the school.
- Not tell anyone about school user names and passwords, not even my best friends.
- Not use other people's work or ideas without asking their permission. Copyright and intellectual property rights must be respected at all times.
- Not install ANY software onto school computers.
- Treat all equipment with respect (No banging of keyboards and mice).
- Tell a teacher immediately if I see anything I am unhappy with.

I understand:

- That the security of the ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- School may exercise its right by any means to monitor use of school computers and internet, including the interception of emails, instant messaging or any other form of communication.

Use of the Internet

I will:

- Only use websites my teacher has told me about.
- Not tell anyone about any username's and passwords used for accessing websites, not even best friends.
- Only use the internet for school work and homework only.
- Not download ANY software onto school computers.
- Not download images that may cause offense to anyone else.
- Not use public chat rooms or social networking sites (e.g. Facebook, Instagram, Twitter, Snapchat etc.).

Safe use of Internet communication

This section refers to ANY form of internet communication, including email, instant messaging, chat rooms etc.

I will:

- Tell a teacher immediately if I see anything I am unhappy with.
- Tell a teacher immediately if I receive messages I do not like.
- NEVER give personal details about myself, or others to ANYONE on the internet (including names, addresses, telephone numbers, email or any other form of internet communication details).
- Tell a teacher if anyone asks for any personal information or comments about you or another person on the internet.

- NEVER post negative or personal comments about another person on the Internet.
- NEVER agree to meet someone I have spoken to on the Internet.

I understand that I am responsible for the content of any emails, messages or any other form of communication I make on the Internet.

I understand that if I deliberately break any of these rules, I could be stopped from using the schools computers.

Signed: _____ (Parent or Carer) Date _____

On behalf of (Pupil's Name – CAPITAL LETTERS please) _____

Appendix 2:

St Catherine's RC Primary School

Acceptable Use Policy: Staff, Governors and Visitors Agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

	(√)
I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.	
I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.	
I will not allow unauthorised individuals to access email/internet/intranet/network, or other school/LA systems.	
I will not engage in any online activity that may compromise my professional responsibilities.	
I will only use the school approved email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.	
I will not browse, download or send material that could be considered offensive to colleagues.	
I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the head teacher.	
I will not download any software or resources that can compromise the network, or are not adequately licensed. I will not download any software or hardware without consultation with the ICT technician.	
I will not connect a computer, laptop or other device (including USB flash drive), to the network/internet that does not have up-to-date anti-virus software, or without consulting the ICT technician first.	
I will not use personal digital cameras or camera devices (e.g. camera phones) for taking or transferring images of pupils or staff.	
I will use and update the school website in accordance with school/local authority advice.	
I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.	
I agree and accept that any computer or electronic device loaned to me by the school is provided solely to support my professional responsibilities. I agree to log out such equipment using the correct format, in liaison with the ICT technician, and understand the equipment must be returned on time.	
I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using such data at any location.	
I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an	

appropriate authority.	
I will embed e-safety into the ICT curriculum that I teach and will ensure that children have a good understanding of the e-safety information they have been taught *(teaching staff)*.	
I will report any child e-safety concerns to the e-safety officer and head teacher and will also log the information on the Safeguarding Concern Form. I will then follow advice for next steps from the e-safety officer and head teacher (e.g. meeting with parents/carers to discuss concerns)	
I will not give out my personal details, such as mobile phone number or personal email address, to pupils or parents.	
I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.	
Images of pupils and staff will only be taken, stored and used for professional purposes, in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or headteacher.	
I will only access my personal mobile phone during non-contact time, unless in mitigating circumstances cleared by the head teacher, e.g. to contact the school during an educational visit. I will ensure my mobile phone is kept in cupboards or drawers and not available during class contact time. It will be kept on silent class contact time except in an emergency situation with the agreement of the headteacher.	
I will report any accidental access to material which might be considered unacceptable immediately to the e-safety officer, ICT technician and head teacher.	
I understand that computers have a password protected screensaver and that I should ensure that computers I use should be fully logged off or the screen locked before being left unattended.	
I understand that the school internet must only be used for school business.	
I understand that all internet and network usage can be logged and this information could be made available to my manager on request.	

User signature

- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I understand that I have the same obligation to protect school data when working on a computer outside school.
- I agree to abide by all the points above.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____ **Date:** _____

Full Name: _____ *(printed)*

Job Title: _____