



ST. THOMAS MORE CATHOLIC PRIMARY SCHOOL

ICT ACCEPTABLE USE POLICY

MISSION STATEMENT

I have come so that they may have life and have it to the full - John 10:10

As a Catholic school, God is at the heart of all we do. We believe that each person is made in His image, deserving to be treated with respect and dignity.

Showing respect, love and care for everyone and everything, we aim to develop harmony between pupils, parents, the school and Parish and grow as a Christian community.

We aim to embed the virtues in every child to believe in themselves to be the best that they can be and leave school as well-rounded individuals who care about themselves, others, and the world.

This policy must be read in conjunction with the
Safeguarding Policy, Online Safety Policy, Relationships and
Behaviour Policy, Curriculum Policy, Data Protection, Complaints Policy
and Security Policy.

Date drafted: February 2026

Date ratified by the Governing Body: February 2026

Date for review by Staff and Governors: February 2027

St. Thomas More Catholic Primary School

Lewis Road | Cheltenham | Gloucestershire | GL51 0HZ

Head Teacher: Mrs K Turner

Tel: 01242 513339 | Fax: 01242 257402 | Email: admin@st-thomasmore.gloucs.sch.uk

www.st-thomasmore.gloucs.sch.uk

Online-safety encompasses Internet technologies and electronic communications including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of Digital technologies within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Live streaming
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality e.g. I Pads
- AI – Artificial Intelligence

It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's Online-safety Policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

End to End Online-safety

Online-safety depends on effective practice at a number of levels:

- Responsible use of information and digital technologies by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Online-safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the South West Grid for Learning (SWGFL) including the effective management of SWGFL filtering.
- National Education Network standards and specifications.

School Online Safety Policy

1. Writing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for Computing, Bullying and for Child Protection/Safeguarding.

- The school will appoint an Online Safety Leader. Our Online Safety Policy has been written by the school, building on government guidance. It has been agreed by Senior Leaders and approved by Governors.
- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy was revised by: S.Cerikan
- It was approved by the Governors in: June 2025

2. Foundation Concepts

- 2.1** Access to information and digital technologies and computer networks owned by St Thomas More Catholic Primary School and access to the internet and e-mail using these resources is conditional on observance of the following Rules for Responsible Use of Information and Digital Technologies (see Appendix 3a and 3b).
- 2.2** The Rules for Responsible Use of Information and Digital Technologies have been written by the School's Computing Subject Leader, building on government guidance. They have been agreed by the school's senior staff and approved by Governors and will be reviewed annually.
- 2.3** It is the policy of the school that access to information and digital technologies, computer networks, the internet and e-mail is provided to staff and pupils as a privilege rather than a right. This privilege may be withdrawn at any time in line with these rules.
- 2.4** The Rules for Responsible Use of Digital Technologies apply at all times to all users, in and out of school hours, whilst using school equipment.
- 2.5** It is an expectation that St Thomas More Catholic Primary School's Computing resources are to be used in a reasonable, efficient, ethical, moral, and legal manner in accordance with the Mission Statement, values, understandings and beliefs of the school.
- 2.6** All staff will have regular online safety training alongside safeguarding training through ME Learning.
- 2.7** Children will have online safety updates that link with the school Curriculum. This will be delivered by school staff and external professionals annually. The school will be responsive in educating the children according to the needs of the cohort and in response to incidents that occur.

3. General Rules

- 3.1** Access to Computing resources will only be provided to staff and pupils who have read and agreed in writing to abide by the Rules for Responsible Use of Information and Digital Technologies. In the case of pupils, parent / guardian permission will also be required.
- 3.2** Users of the school's computer systems are allowed to use the facilities freely for school work.
- 3.3** Individual users of school computing resources are responsible for their own behaviour and actions.
- 3.4** Use of school computing resources including e-mail is not considered to be private and should not be treated as such. School senior staff may monitor computer usage at any time with or without the user's knowledge.
- 3.5** School computing resources are provided for academic use and may not be used for any form of personal business or financial gain.

4. Network Access / Basic Computer Security

- 4.1** Users must access the system using only usernames and class work areas that have been assigned to them. Users are personally responsible for the security of resources and passwords issued to them.
- 4.2** Users must not allow anyone else to access the system using a user name, password or resource issued to them. Computer screens should be locked or on a timer if left unattended by staff. Users are reminded that if this situation occurs they may be charged with illegal actions carried out by the third party.

- 4.3** Users must not attempt to access the system using someone else's username or password or try to access class areas, resources or facilities which have not been made available to them. Hacking" is illegal under the Computer Misuse Act.
- 4.4** Any user who becomes aware of a breach of network security, loophole or a breach of the Rules for Responsible Use of Information and Digital Technologies is required to inform the Staff immediately.
- 4.5** **Securus has been installed by IT Services this academic year.**

5. Physical Behaviour & Care of Equipment

- 5.1** Users must not cause any unnecessary noise or disturbance to others, or use facilities in a way that results in degradation or disruption of the service to others. Playing and holding conversations creates noise and stops others using the resources to their full potential.
- 5.2** Users must not eat or drink when using or near Computing resources.
- 5.3** Users must treat with care and respect equipment and resources within the school and at other sites accessed through school facilities. Malicious action or vandalism will result in immediate suspension from school facilities. Never deliberately damage or break anything.

6. Software Usage

- 6.1** Software provided on computing resources has been carefully selected on the basis of educational value and suitability of content and is subject to strict licensing requirements. For this reason users must not install any software unless previously agreed by the Headteacher or SLT. This includes the downloading of applications and utilities from the internet.
- 6.2** No games of any kind with the exception of approved "edutainment" titles may be used on school computing resources during school hours.
- 6.3** Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.
- 6.4** Computing resources must not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act. Any person wishing to use facilities for such a purpose are required to inform the SLT in advance and comply with any restrictions that the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

Teaching and Learning

7. Why Internet use is important

- 7.1** The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- 7.2** Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

8. Internet use will enhance learning

- 8.1 The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- 8.2 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use as part of their unit Online Safety as well as ongoing learning thread throughout every unit.
- 8.3 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, this will be taught using the Purple Mash Scheme.
- 8.4 Users are not allowed access to public or unregulated chat rooms or to use instant messaging programs.
- 8.5 The school considers all connections to remote locations on the Internet as Virtual School Trips. Therefore, the rules that apply to conduct on regular school trips also apply to users visiting internet sites. It is important that users realise that they are acting as an ambassador for the school.
- 8.6 With the exception of copyright free pictures and text files, no internet content may be downloaded to or via school computing resources by non-staff users. This includes, but is not limited to, music files, games, screen savers, desktop themes and other software.
- 8.7 As computing resources are shared between users and linked to the school address, for their own protection, users are not allowed to use the resources to browse auction sites, make any form of online order or purchase or use internet banking services.

9. Pupils will be taught how to evaluate Internet content

- 9.1 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- 9.2 Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

10. Managing Internet Access Information System Security

- 10.1 School ICT systems capacity and security will be reviewed regularly.
- 10.2 Virus protection will be updated regularly.

11. E-mail

- 11.1 Members of staff will be issued with their own email account.
- 11.2 Users may not use other e-mail accounts on the school system.

12. Published Content and the School Website

- 12.1 The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- 12.2 The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

13. Child Protection

- 13.1 Photographs that include pupils will be selected carefully and pictures will not be used of individual pupils who do not have permission for the web.
- 13.2 Pupils' full names will not be used anywhere on the Website, Blog or photographs where permission has not been granted.

- 13.3** Written permission from parents or carers will be obtained before photographs of pupils or pupil's work are published on the school Web site and these records will be kept at the office.
- 13.4** It is essential that children are safeguarded from potentially harmful and inappropriate material. When monitoring and educating about online safety, the areas we will focus on are:
- a)** Content: exposure to illegal, inappropriate or harmful content, for example pornography, fake news, racism, misogyny, self-harm, suicide and extremism.
 - b)** Contact: being subjected to harmful online interaction with other users, for example peer to peer pressure, commercial advertising and adults posing as children with the intention to groom.
 - c)** Conduct: personal online behaviour that increases the likelihood of or causes harm, for example making, sending and receiving explicit images online bullying.
 - d)** Commerce: risks such as online gambling, inappropriate advertising, phishing or financial scams.

14. Social Networking and Personal Publishing

- 14.1** The school will block/filter access to social networking sites.
- 14.2** Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- 14.3** Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils and regular reminders will be sent in the newsletter.
- 14.4** Online-safety information evenings will be held on an annual basis in association with the police, when possible.

15. Managing Filtering

- 15.1** The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- 15.2** If staff or pupils discover an unsuitable site, it must be reported immediately to the class teacher and to the Online-safety Subject Leader.
- 15.3** Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

16. Managing Emerging Technologies

- 16.1** Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- 16.2** Mobile phones will not be allowed in school by pupils unless previously agreed by the Headteacher because children need it for walking home alone. At these times it is off as soon as they enter the school site and then handed to their teacher who will place it into their desk drawer. Whilst teachers will take every possible care to keep the phone safe, the school and/or teachers are not to be held responsible for it. Staff must restrict mobile phone use to outside the classroom and when taking pupils off site.

17. Protecting Personal Data

- 17.1** Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

18. Anti-Virus Precautions

- 18.1** A computer virus is a malicious parasitic program written to alter the way that computers operate without permission or knowledge. They can destroy data, display inappropriate messages or destroy functionality. All school ICT resources are equipped with anti-virus software but home users may not have this, or have an inadequate level of protection.
- 18.2** Viruses spread by copying themselves to other computers via discs as they are loaded on an infected system. For this reason users are not allowed to transfer files to and from school systems and their own equipment by any means other than an encrypted USB which belongs to the school.
- 18.3** Viruses and mal-ware are also spread by attachments on e-mails. Users receiving mail carrying attachments from unknown users or from a known user with an unusual subject line such as "I love you" or "click me" should delete the message without opening it.
- 18.4** The final source of malicious software is internet downloads and pop ups. While most such items will be blocked by the school's filtering system, users should be aware of the existence of these pop ups and avoid clicking on or activating them.
- 18.5** Any deliberate attempt by a user to introduce virus, mal-ware or similar software will be treated in the same way and with the same severity as physical vandalism to school equipment.

19. Policy Decisions

- 19.1** Authorising Internet access
- 19.2** All staff (including volunteers) must read and sign the 'Online safety /Acceptable Use Policy before using any school computing resource.
- 19.3** The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- 19.4** Access to the Internet will be adult led with directly supervised access to specific, approved on-line materials.

20. Assessing Risks

- 20.1** The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.
- 20.2** The school will audit computing provision to establish if the Online-safety Policy is adequate and that its implementation is effective.

21. Handling Online-safety Complaints

- 21.1** Complaints of Internet misuse will be dealt with by a senior member of staff.
- 21.2** Any complaint about staff misuse must be referred to the Headteacher.
- 21.3** Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and immediately reported to the Designated Safeguarding Lead.
- 21.4** Pupils and parents will be informed of the complaints procedure.

22. Communications Policy

Introducing the Online-safety Policy to Pupils

- 22.1** Online-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and on Internet Safety Day.
- 22.2** Pupils will be taught Online-safety in specific lessons within PSHCE, RSHE and each year group is taught Online-safety focused sessions within their computing curriculum, following the school's scheme of work using educational websites for support such as think know, childnet and kidscape, etc. Online safety is also threaded through all computing lessons.
- 22.3** Pupils will be informed that network and Internet use will be monitored.

23. Staff and the Online-safety Policy

- 23.1** All staff will be given the School Online-safety Policy and its importance explained.
- 23.2** Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

24. Enlisting Parents' Support

- 24.1** Parents' attention will be drawn to the School Online-safety Policy in newsletters, the School Prospectus and on the school Website.

25. Copyright

- 25.1** Users must not take information from the Internet and pass it off as their own work (plagiarism).
- 25.2** Users must not publish information on the school or other websites that is protected by copyright.
- 25.3** No user may copy programs or data which are copyright or subject to restrictive licence agreements on to removable media or on to computers' hard discs. Users should assume that

ALL software is subject to such a restriction.

26. Good Practice

- 26.1** Storage space on the network is limited and all users are requested to ensure that old, unwanted data is removed from their area. Users unsure of what can safely be deleted should ask the Network Manager for advice.
- 26.2** Computing resources are backed up every evening automatically. This means files can be restored if deleted or lost in error. However, if users create and delete files on the same day then a backup will not be available to restore. Copies of particularly important files should be saved on removable media until the evening backup is complete.
- 26.3** Users should save their work regularly (approximately every 15 minutes). The network is very reliable but problems do occur (programs crash, power can fail). If you save your work regularly and the network does fail for any reason, you will have only lost approximately 15 minutes work.

27. Use of Computing Resources Out Of School

- 27.1** Certain users may be allocated computing resources for use outside of school. Equipment so issued is the responsibility of the user to which it is assigned and may be used by that user only. Use by family and friends is not permitted.
- 27.2** When used off school premises, computing resources and their users are still covered by all of the Rules for Responsible Use of Information and Digital Technologies including those relating to the installation of software, use of the internet and e-mail.
- 27.3** In exception to 27.2 (above) a user allocated a school laptop may set up a basic dial-up or broadband connection on the machine to allow internet access from home subject to the other Rules for Responsible Use of Information and Digital Technologies so long as this does not interfere with the systems operation on the school network. Machines so used will be provided with firewall and anti-malware software to help protect them when used outside of the school's filtered internet environment.
- 27.4** In exception to 27.2 (above) a user allocated a school laptop may install printer driver software necessary to allow use of a home printer so long as this does not interfere with the systems operation on the school network.
- 27.5** Staff who have been trained, may access the school server remotely. The same rules above apply. Remote access should only be via a school device, such as laptop. The connection should be logged off at the end of each remote access session.

28. Disciplinary Action

- 28.1** Any infringement of Rules for Responsible Use of Information and Digital Technologies may lead to temporary or permanent suspension of use of Computing resources, internet access or both.
- 28.2** Any alleged infringement will be investigated by the Computing Subject Leader or SLT who can, within their discretion, waive or apply a penalty as the circumstances warrant.
- 28.3** Where the Computing Subject Leader takes the view that it is a particularly serious case, multiple offences have occurred or the possibility of a criminal offence exists, the matter will be referred to the Headteacher and Governing Body. If it is agreed that it warrants such action, formal disciplinary proceedings will be initiated.

29. Understanding Cyber bullying

- 29.1** Cyber bullying is the use of electronic communication to abuse another person.
- 29.2** It can take place anywhere and involve few or many people.
- 29.3** Anybody can be targeted including pupils and school staff.
- 29.4** It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorized publication of private information or images etc.

30 Procedures to Prevent Cyber bullying

- 30.1** Staff, pupils, parents and Governors to be made aware of issues surrounding cyber bullying and are fully aware of Keeping Children Safe In Education 2025.
- 30.2** Pupils and parents will be urged to report all incidents of cyber bullying to the school.
- 30.3** Staff CPD will assist in learning about current technologies
- 30.4** Pupils will learn about cyber bullying through online safety lessons, PSHE, RSHE, assemblies, anti-bullying week activities and other curriculum projects. Visiting speakers will deliver some of this learning.

- 30.5** Staff, Governor and Visitors will sign an Acceptable Use Agreement/Code of Conduct (**Appendix 1**).
- 30.6** Parents will be provided with information and advice on how to combat cyber bullying.
- 30.7** Parents and pupils will be expected to sign an Acceptable Use of Information and Digital Technologies agreement after discussing its meaning with their children (**Appendix 4a**).

31. Online Vulnerability

- 31.1** Procedures to be followed in instances where children have been vulnerable online because of online contact, conduct or commerce can be found within the safeguarding policy.

Appendix 1

St Thomas More Catholic Primary School

Acceptable Use Agreement: All Staff, Volunteers and Governors
--

This agreement covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, 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 not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, or any system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the school's approved email system for any school business.
- I will only use the approved email and 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 or equipment failure to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other ICT 'defence' systems.
- If I use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff engaged in school activity, I will ensure these are transferred to the school system by the end of the day and deleted from my device.
- Wherever possible I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system within school.
- I will adhere to the E-Safety policy on use of mobile phones / devices at school
- I will use the school's Learning Platform in accordance with school protocols.
- 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 will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role as detailed in Appendix 6.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- 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 any such data at any location.
- I understand that data protection policy requires that any information seen by me about 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 alert the schools named child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I will only use any LA system I have access to in accordance with their policies.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a named child protection officer at the school.
- I understand that all Internet and network traffic / usage can be logged, and this information can be made available to the Head / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- Staff that have a teaching role only which includes Teaching Partners working with children: I will embed the school's Online Safety / digital literacy curriculum into my teaching.
- I will follow the procedures set out in Appendix 6 relating to my use of social network sites.

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others Online safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature Date.....

Full Name (printed)

Job title / Role

Appendix 2

St Thomas More Catholic Primary School

Guidance: What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the Head Teacher/~~E-safety~~ Computing Lead / DSL and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered.

An inappropriate website is accessed intentionally by a child.

1. Refer to the Acceptable Use Agreement that was signed by the child, and apply agreed sanctions.
2. Notify the parents/carer of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An inappropriate website is accessed intentionally by a staff member.

1. Ensure all evidence is stored and logged
2. Refer to the Acceptable Use and Staffing Agreement that was signed by the staff member and apply disciplinary procedure.
3. Notify Head Teacher who will notify Chair of Governors.
4. Inform the school technicians and ensure the site is filtered if need be.
5. In an extreme case where the material is of an illegal nature:
 - a. Contact the local police and follow their advice.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the Head Teacher (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the Head Teacher should then:
 - Remove the device to a secure place.
 - Instigate an audit of all ICT equipment by the school's ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
 - Identify the precise details of the material.
 - Take appropriate disciplinary action (undertaken by Head Teacher).
 - Inform the Chair of Governors of the incident.
4. In an extreme case where the material is of an illegal nature:
 - The Head Teacher will contact the local police and follow their advice.
 - If requested to remove the device to a secure place and document what they have done.

All the above incidences must be reported immediately to the Head Teacher and E-safety Co-ordinator.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including E-safety Anti-Bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's email service provider if known.
5. Notify parents/carers of all the children involved.
6. Consider delivering a parent workshop for the school community.

7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection)

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. The Head Teacher will inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Chair of Governors etc).

The school may wish to consider delivering a parent/carer workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP <http://www.ceop.gov.uk/>
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that the technical team block access to the game
4. Consider the involvement of social services and child protection agencies.
5. Consider delivering a parent/carers workshop for the school community.

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

The Head Teacher will:

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact Chair of Governors and Friends of St Thomas More
4. Consider delivering a parent/carers workshop for the school community.

All of the above incidences must be reported immediately to the Head Teacher and E-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.



Appendix 3a

St Thomas More Catholic Primary School

Key Stage 2 Rules for Responsible ICT Use



Keeping safe: stop, think, before you click!

These rules will keep everyone safe and help us to be fair to others:

- I will only use the school's computers for school work and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my login and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not visit Internet sites I know to be banned by the school.
- I will only email people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- I will not use AI to manipulate pictures or data that may cause harm or offence to another person.

I agree to follow these Rules for Responsible ICT Use and am aware of the consequences if I do not follow them.

Name:

Date:

Appendix 3b



St Thomas More Catholic Primary School

Key Stage 1 Rules for Responsible ICT Use



Keeping safe: stop, think, before you click!

These rules will keep everyone safe and help us to be fair to others:

- I will only use the Internet and email with an adult.
- I will only use Internet sites chosen for me by an adult.
- I will keep my login and password secret.
- I will only send polite and sensible emails.
- I will not give out my name, home address, phone number, school details or any other personal information about myself online.
- I know who I can trust when I am on the Internet and will tell my teacher if anything makes me feel uncomfortable.
- If I see anything I am unhappy with or I receive a message I do not like, I will tell my teacher.

I agree to follow these Rules for Responsible ICT Use and am aware of the consequences if I do not follow them.

Name: _____

Date: _____



Appendix 4a

Online safety agreement form: parents/carers

Parent / Carer name: _____

Pupil name: _____

As the parent/carers of the above pupil, I grant permission for my daughter/son to have access to use the Internet and other ICT facilities at school.

I know that my daughter/son has signed an Online safety agreement form and that they have a copy of the St Thomas More Catholic Primary School's Rules for Responsible ICT Use.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching Online safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their Online safety or behaviour that they will contact me. Appropriate sanctions may be imposed.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's Online safety.

Parent / Carer signature: _____

Date: ____/____/____

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / Carer signature: _____ **Date:** ____/____/____

Appendix 4b



Use of digital images - photography and video

To comply with the Data Protection, Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to store photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.
- Your child's image for presentation purposes around the school;
e.g. in school wall displays and PowerPoint® presentations to capture images around the school or in the local area as part of a project or lesson.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents/carers, schools or educators;
e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Appendix 5



St Thomas More Catholic Primary School

Policy: How will infringements be handled?

Whenever a pupil or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher or if the Head Teacher is involved by the Chair of Governors and will reflect the school's behaviour and disciplinary procedures.

The following are provided as **exemplification** only:

PUPIL	
Category A infringements	Possible Sanctions:
• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	Refer to class teacher / pupil Escalate to: senior manager / Online Safety Coordinator
Category B infringements	Possible Sanctions:
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups • Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc • Trying to buy items over online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it	Refer to Class teacher/ E-safety Coordinator Escalate to: Head Teacher removal of Internet access rights for a period / removal of phone until end of day / contact with parent

PUPIL	
Category C infringements	Possible Sanctions:
- Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. - Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) - Trying to access offensive or pornographic material (one-off) - Purchasing or ordering of items online - Transmission of commercial or advertising material	Refer to Class teacher / E-safety Coordinator / Head teacher / removal of Internet and/or Learning Platform access rights for a period Escalate to: Head Teacher contact with parents/ carer and removal of equipment Other safeguarding actions if inappropriate web material is accessed: Ensure appropriate technical support filters the site
Category D infringements	Possible Sanctions:
- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned - Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent - Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 - Bringing the school name into disrepute	Refer to Head Teacher / Contact with parents/carers Other possible safeguarding actions: - Secure and preserve any evidence - Inform the sender's email service provider. - Liaise with relevant service providers/ instigators of the offending material to remove - Report to Police / CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	Possible Sanctions:
- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. - Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. - Not implementing appropriate safeguarding procedures. - Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. - Misuse of first level data security, e.g. wrongful use of passwords. - Breaching copyright or license e.g. installing unlicensed software on network.	Referred to: Head Teacher <i>Warning given if appropriate in line with the Disciplinary Policy</i>
Category B infringements (Gross Misconduct)	Possible Sanctions:
- Serious misuse of, or deliberate damage to, any school / Council Trust computer hardware or software; - Any deliberate attempt to breach data protection or computer security rules; - Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; - Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; - Bringing the school name into disrepute	Referred to Head Teacher / Chair of Governors; Other safeguarding actions: - Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. - Instigate an audit of all ICT equipment by an outside agency, such as the school's ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. - Identify the precise details of the material. Report to LA/LSCB and Human resource. Report to Police / CEOP where child abuse or illegal activity is suspected.

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended**, and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

<https://www.ceop.police.uk/Safety-Centre/>

<http://www.iwf.org.uk>

How will staff and pupils be informed of these procedures?

- They will be fully explained and included within the school's E-safety Policy. All staff will be required to sign the school's Online safety Acceptable Use Agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents, so they can develop 'safe behaviours'. Pupils will sign an age appropriate Online safety / acceptable use agreement form;
- The school's Online safety Policy will be made available and explained to parents/carers, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on Online safety issues.

Appendix 6



Social Networking

School Principles:

This policy relates to social networking activities such as:

- Blogging (writing personal journals to publicly accessible internet pages).
- Social networking sites such as Facebook, Instagram, Snapchat MySpace or Bebo and others
- The posting of material, images or comments on websites such as You Tube
- Online discussion forums,
- Collaborative spaces,
- Media sharing
- 'Microblogging' applications such as Twitter
- MSN,
- Virtual Worlds.

The dangers inherent in these activities include:

- Potential negative effect on the school's reputation or image.
- Compromising the school's commitment to safeguarding children
- Breaching school confidentiality procedures.
- Staff grievances leading to disciplinary cases.
- School leaders and governors are exposed to legal risks

This policy has been written to set out the key principles and staff code of conduct with the use of social networking sites.

Staff Procedures:

1. All staff have a responsibility to ensure that they protect the reputation of the school and treat colleagues and members of the school community with professionalism and respect.
2. It is important to protect all staff and members of our community from allegations and misinterpretations which can arise from the use of social networking sites.
3. Safeguarding children is a key responsibility of all members of staff and it is essential that staff act responsibly if they are using social networking sites out of school.
4. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.
5. Blogging and accessing social networking sites at work using school equipment is not permitted.
6. The use of the school's name, logo, or any other published material without written prior permission from the Head Teacher
7. No communications irrespective of their anonymity should be shared that relate to any specific event, protocol, pupil or person at School.
8. All information shared through social networking applications, even via private spaces is subject to copyright, data protection and Freedom of information legislation & the Safeguarding Vulnerable Groups Act 2006.
9. School staff must not invite, accept or engage in communications with parents or children from the school community to any personal social networking sites.

10. Any communication received from children to School Representatives must be immediately reported to the Head Teacher – Designated Child Protection Officer and procedures for safeguarding followed.
11. If a School Representative is made aware of any other inappropriate communications involving any child and social networking. These must be reported immediately as above.
12. School internet policy must be used at all times when children use ICT and access the internet in school.

School Action:

Breach of the policy could result in:

- Staff being suspended.
- The closure of any applications or removal of content which may adversely affect the reputation of the School or put at risk of legal action.
- Misconduct or gross misconduct procedures to which the school and Local Authority Dismissal and Disciplinary Policies apply.