



ST. THOMAS MORE CATHOLIC PRIMARY SCHOOL

E-SAFETY 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 and Child Protection Policy and Acceptable User Policy

Date drafted: June 2025

Date ratified by the Governing Body: June 2025

Date for review by Staff and Governors: June 2026

St. Thomas More Catholic Primary School

Lewis Road | Cheltenham | Gloucestershire | GL51 0HZ

Head Teacher: Mrs N Tippen

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

www.st-thomasmore.gloucs.sch.uk

CONTENTS

1. Introduction and Aims

- Rationale and aims
- Roles and responsibilities

2. Teaching and Learning

- Pupil E-safety curriculum
- Staff and governor training
- Parent/Carer awareness and training

3. Safeguarding

- How the policy is communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring
- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing
- Learning Platforms

Data Security

- Management Information System access
- Data transfer

Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)
3. Acceptable Use Agreement including photo/video permission (Parents/Cares)
4. Protocol for responding to E-safety incidents
<http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx> - handling infringements
<http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf> - page 23 onwards
5. Protocol for Data Security
6. Search and Confiscation guidance from DfE
<https://www.gov.uk/government/publications/searching-screening-and-confiscation>

1. INTRODUCTION AND AIMS

Introduction

This policy applies to all members of St Thomas More Catholic School community (including staff, governors, pupils / pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both in and out of St Thomas More Primary School.

In England, the Department for Education (DfE) provides the key guidance for schools and colleges through 'Keeping Children Safe in Education' (DfE, 2024)¹. It sets out the legal duties to safeguard and promote the welfare of children and young people under the age of 18 in education settings. As of September 2024, the guidance also provides detailed information on how schools and colleges should respond to sexual violence and harassment between children. Furthermore, Schools and colleges must also follow the guidance set out in Working Together to Safeguard Children (DfE, 2023).

The safeguarding duty of schools is set out in section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014, and the Non-Maintained Special Schools (England) Regulations 2015.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-safety behaviour that take place out of school.

Aims

The aim of this policy is to:

- Set out the key principles expected of all members of the school community at St Thomas More with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of St Thomas More Catholic Primary School
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Roles and Responsibilities

Role	Key Responsibilities
Senior Leadership Team (DSL)	• To take overall responsibility for E-safety provision • To take overall responsibility for data and data security • To ensure that all data held on pupils on the school office machines have appropriate access controls in place • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their E-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious E-safety incident. • To receive regular monitoring reports from the E-Safety Lead • To ensure that there is a system in place to monitor and support staff who carry out internal E-safety procedures (e.g. network manager) • Educating Parents/Carers and raising awareness

Role	Key Responsibilities
The Computing Lead will act as E-Safety Lead (in conjunction with DSL)	• Takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies / documents • Promotes an awareness and commitment to E-safety throughout the school community • Ensures that E-safety education is embedded across the curriculum • Liaises with school ICT provider • To communicate regularly with SLT and the designated Computing/E-safety Governor to discuss current issues. • To ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident • Facilitates training and advice for all staff • Liaises with the Local Authority and relevant agencies • Is regularly updated in E-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Computing/E-safety Governor	• To ensure that the school follows all current E-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governing Board receiving regular information about E-safety incidents and monitoring reports. A member of the Governing Board has taken on the role of Computing/E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in E-safety activities • The role of the Computing/E-Safety Governor will include: • Regular review with the E-Safety Co-ordinator.
Computing Lead	• To oversee the delivery of the E-safety element of the Computing curriculum • To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected • To report any E-safety related issues that arises, to the E-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis • That he / she keeps up to date with the school's E-safety policy and technical information in order to effectively carry

Role	Key Responsibilities
	out their E-safety role and to inform and update others as relevant • To keep up-to-date documentation of the school's E-security and technical procedures
Teachers	• To embed E-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
Staff	• To read, understand and help promote the school's E-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • To be aware of E-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies about these devices • To report any suspected misuse or problem to the E-safety coordinator • To maintain an awareness of current E-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Staff	• To read, understand and help promote the school's E-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • To be aware of E-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies about these devices • To report any suspected misuse or problem to the E-safety coordinator • To maintain an awareness of current E-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy (KS1 it would be expected that parents / carers would sign on behalf of the pupils) • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand-held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of E-safety policies
Parents/carers	• To support the school in promoting E-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Agreement prior to using any equipment or the Internet within school

2. Teaching and Learning

Pupil E-safety curriculum

This school

- Has a clear, progressive E-safety education programme as part of the Computing curriculum / PSHE curriculum. The school uses The Oak National Academy to deliver a comprehension E-Safety package that follows a carefully planned progression from Year 1 to Year 6. EYFS support the teaching of E-safety through the seven areas of learning. In addition to The Oak National Academy, E-Safety is supported by Thinkuknow and The SMART Rules. This covers a range of skills and behaviours appropriate to their age and experience, including:
 - to STOP and THINK before they CLICK
 - to develop a range of strategies to evaluate and verify information before accepting its accuracy;

- to be aware that the author of a web site / page may have a bias or purpose and to develop skills to recognise what that may be;
 - to know how to narrow down or refine a search;
 - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
 - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
 - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
 - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
 - to understand why they must not post pictures or videos of others without their permission;
 - to know not to download any files – such as music files - without permission;
 - to have strategies for dealing with receipt of inappropriate materials;
 - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
 - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
 - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
 - Plan for pupils attend E-safety assemblies and talks with PCSO and well as celebrating Safer Internet Day
 - Will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign/copies will be sent home for parents/carers to see/will be displayed throughout the school (*Appendix 3a and 3b*).
 - Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
 - Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright / intellectual property rights;
 - Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
 - Are reactive to safeguarding concerns that arise through E-safety issues and put in place interventions or lessons in response.
 - Pupils are given the opportunity to comment on relevant issues through the school council.

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

- Makes training available to staff and governors on E-safety issues and the school's E-safety curriculum
- Provides, as part of the induction process, all new staff and governors [including those on university/college placement and work experience] with information and guidance on the E-safeguarding policy and the school's Acceptable Use Policies (*Appendix 1*), copies of the Guidance (*Appendix 2*), copies of pupil's rules (*Appendix 3a and 3b*), copies of Parents' Agreement Form and Use of Digital Images (*Appendix 4a and 4b*), Infringements procedures (*Appendix 5*) and Social Networking procedures (*Appendix 6*)

Parent/Carer awareness and training

This school

- Parents/carers will be asked to read and sign the Acceptable Use Policy parent agreement and Use of Digital Images forms as their child enters the school (*Appendix 4a and 4b*).
- Runs a rolling programme of advice, guidance and training for parents, including:
 - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of E-safe behaviour are made clear
 - school prospectus; in school newsletters; on the school web site;
 - demonstrations, practical sessions held at school;
 - suggestions for safe Internet use at home;
 - provision of information about national support sites for parents
 - communicates through 'Class Dojo' recent E-safety articles or needs of the school.

3. Safeguarding

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign before being given access to school systems. (KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- are expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff/Governors

- are responsible for reading the school's E-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand-held devices.

Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- are not allowed mobile phones in school

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the E-safety acceptable use agreement form at time of their child's entry to the school
- are made aware of what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the E-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely a need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with E-safety issues
- monitoring and reporting of E-safety incidents takes place and contribute to developments in policy and practice in E-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / GCSP through CPOMS.
- parents / carers are specifically informed of E-safety incidents involving young people for whom they are responsible.
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LA and so connects to the 'private' National Education Network;
- Uses the Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils;
- Ensures network healthy through use of anti-virus software network set-up so staff and pupils cannot download executable files;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct pupils to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , KIDDLE
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that they must report any failure of the filtering systems directly to the person responsible for URL filtering.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's E-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
We provide pupils with a collective network log-in username.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff accessing LA systems do so in accordance with any school policies; e.g. email or Intranet, GCC website documentation etc.
- Maintains equipment to ensure Health and Safety is followed;
e.g. equipment installed and checked, projector filters cleaned by approved supplier / electrical engineers.
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);

- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

This school

- Provides staff with an email account for their professional use, Outlook Mail and makes clear personal email should be through a separate account;
- Will contact the police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Staff:

- Staff can only use the Outlook email systems on the school system
- Staff only use the email systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer full staff or pupil personal data but use initials and agreed codes.
- Staff know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
 - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
 - the sending of chain letters is not permitted;
 - embedding adverts is not allowed;

- All staff sign to say they have read and understood the E-safety rules, including email and we explain how any inappropriate use will be dealt with.

School website

- The Senior Leadership Team takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained;
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published, or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual email identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers to update their class pages regularly.

Social networking

School staff and governors will ensure that in private use:

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

Video Conferencing

- Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer.
- External IP addresses should not be made available to other sites.
- Only web based conferencing products that are authorised by the school (and are not blocked by internet filtering) are permitted for classroom use.
- Videoconferencing is supervised directly by a teacher. In the event of this not being the case pupils must ask permission from the teacher before making or answering a videoconference call.
- Permission for pupils to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in the school. Only where permission is granted may pupils participate.
- Only key administrators have access to videoconferencing administration areas.

Learning Platform

Teachers monitor the use of the learning platform's (Mathletics/TT Rockstars/Spelling Frame/Mathseeds) by pupils regularly during all supervised sessions, but with particular regard to messaging and communication.

Staff use is monitored by the administrator.

User accounts and access rights can only be created by the VLE administrator.

Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to the learning platform.

When staff, pupils, etc leave the school their account or rights to specific areas will be disabled (or transferred to their new establishment if possible / appropriate).

Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the learning platform may be suspended for the user.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carer may be informed.

A visitor may be invited onto the learning platform by the administrator following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

Teachers use Class Dojo as a communication platform to encourage children and to get parents/carers engaged in their children's learning. This platform's sole purpose is to

The school also uses an online music (Charanga), Art and DT (KAPOW), computing (Oak National Academy), learning for life (SCARF) and language (Language Angels) platform to deliver lessons. These online platforms are solely used by teachers and are monitored by the Computing Lead. No data or information is held on the learning platforms.

Strategic and operational practices

At this school:

- The Assistant Headteacher (Susan Cerikan) is the GDPR Lead (General Data Protection Regulations).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners in a spreadsheet.
- We ensure staff know who to report any incidents to where data protection may have been compromised.
- All staff are DBS checked and records are held in one Single Central Register (SCR) which is password protected by the School Bursar. There is also a printed spreadsheet available always for checking and inspection.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
 - staff,
 - governors,
 - pupils
 - parents/carers

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure areas on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- Back-ups are encrypted
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.
- We are using secure file deletion software.

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupil's & parents/carers or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head Teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head Teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents/carers need to contact children during the school day, they should do so only through the School's office. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent always.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Pupil's use of personal devices

- The school does not allow pupil mobile phones to be brought into school unless they are a year 5 or 6 child and have permission to walk home. In this case, children are able to bring a mobile phone to school as a security measure. The phones must be switched off when on school premises and handed to the class teacher immediately. The mobile will only be returned at the end of the school day.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device in school and deleted before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Agreement, and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their E-safety education programme and taught to consider how to publish for a wide range of audiences which might include governors, parents/carers or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with

images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

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 TAs working with children: I will embed the school's E-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 E-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 E-safety policies.

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

Signature Date.....

Full Name (printed)

Job title / Role

Authorised Signature (Head Teacher)

I approve this user to be set-up on the school systems relevant to their role

Signature Date

Full Name (printed)

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 Lead 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 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

E-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 E-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 E-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 E-safety or E-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 E-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 E-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 / E-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 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

<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 E-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 E-safety / acceptable use agreement form;
- The school's E-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 E-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, 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.