St Thomas More Primary School
E Safety & Acceptable Use Policy
Reviewed every three years

Reviewed	Agreed by GB	Next review
July 2017	July 2017	Autumn 2020
November, 2020 FGB	November 2020	Autumn 2023
November, 2023	November 2023	Autumn 2026

St Thomas More is committed to promoting and respecting the health, safety and welfare of all our children and any adults who work in our school

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix C), and ensuring that pupils follow the school's terms on acceptable use (appendix A and B)

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by alerting the Headteacher and reporting it to LGFL and IT support
- Following the correct procedures by reporting to the Headteacher and then making IT support aware if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

E–Safety and acceptable use policy

E-Safety covers issues relating to pupils as well as adults and their safe use of the Internet, mobile phones, devices and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children and relating to keeping children safe in education document.

The School Policy has been agreed by the Senior Leadership Team and the Governing Body. The e–Safety and Acceptable Use Policy and its implementation will be reviewed every three years.

The e-Safety Policy operates in conjunction with other policies including Safeguarding and Child Protection Policy, The Prevent Duty, School Discipline and Pupil Behaviour Policy (including Anti-Bullying Policy) and Remote Learning Policy.

Introduction

Usually, the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and

evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher. There is therefore a genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- *establish the ground rules we have in school for using the Internet;*
- *describe how these fit into the wider context of our discipline policy;*
- *demonstrate the methods used to protect the children from sites containing pornography, racist or politically-extreme views and violence.*

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

At St Thomas More, we feel that the best recipe for success lies in a combination of site-filtering, supervision and by fostering a responsible attitude in our pupils in partnership with parents. Children must have returned and signed a consent form before being allowed to use the ICT facilities that involve accessing the internet.

Teaching and learning

Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The use of the names of children or photographs of children for websites will require written permission from parent(s)/carer(s) included on the consent form. If a picture is placed on the website the child's full name will not be displayed.

Internet use enhances learning

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. St Thomas More Primary School ensures that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

Pupils are taught how to evaluate Internet content

Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.

Using the Internet for Education

The benefits include:

- *access to a wide variety of educational resources including libraries, art galleries and museums*
- *rapid and cost effective world-wide communication;*
- *gaining an understanding of people and cultures around the globe;*

- staff professional development through access to new curriculum materials, expert knowledge and practice;
- exchange of curriculum and administration data with LA/DfE;
- greatly increased skills in literacy, particularly in being able to read and appraise critically and then communicate what is important to others

The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons. All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught and the ICT subject leader will assist in the dissemination of this information. Initially the pupils may be restricted to sites which have been reviewed and selected for content. They may be given tasks to perform using a specific group of web sites.

Expectations of Pupils using the Internet

Pupils are expected to read and agree the Internet Agreement. At St Thomas More Primary School, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.
- Pupils are expected not to use any inappropriate language in their email communications and contact only people the teacher has approved. They are taught the rules of etiquette in email and are expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- No programs on data-stick should be brought in from home for use in school. This is for both legal and security reasons.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school.
- Pupils must conduct themselves within the parameters of the school rules at all times failure to do so will result in discipline in line with the school's behaviour and discipline policy.

Internet access is a privilege for pupils who show a responsible and mature approach to its use. Unacceptable use of the school system will result in one or more of the following:

a) a ban, temporary or permanent, on the use of the computer facilities at school
b) a letter informing Parents/Carers of the nature of the unacceptable use
c) appropriate restrictions placed on access to school's computer facilities
d) exclusion from school

Pupil Evaluation of Internet Content

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In

particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.
Pupils use age-appropriate tools to research Internet content. The evaluation of online materials is a part of teaching and learning in every subject and is viewed as a whole-school requirement across the curriculum.

Managing Information Systems

St Thomas More Primary School recognises the importance of maintaining its Information Systems in relation to security of provision and unauthorised access to ensure the personal safety of staff and pupils.

The school subscribes to the following rules in relation to its Local Area Network (LAN):

- Users must take responsibility for their network use.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Email management

- All staff have a network account and individual email address.
- Staff will only use official school provided email accounts to communicate with Parents/Carers
- Staff should not use personal email accounts for professional purposes.
- Email sent to external organisations should be written carefully in the same way as a letter written on school headed paper would be.
- The school has a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

Digital images

Digital images, whether still or moving, can make an important contribution to the learning and teaching of our pupils. They also make an invaluable contribution to recording the life and activities of the school community. It is therefore important that, during these processes, staff and pupils avoid issues which may prove to be areas of conflict and potential catalysts for misconduct or offence.

- Digital images or video collected during school activities remain the property of the school.
- Pupils or staff cannot take a copy or transfer images to a portable storage device, or include them as an email attachment without permission of the Head of School.
- Staff or pupils taking images/recordings around the school should notify others of the purpose of their recording, before they capture the images.
- Images of staff or pupils should not be taken without their permission.
- Parents/Carers must give permission for the use of digital images of their child to be used:
    - within the school only (eg on display boards, on screens).
    - within school publicity materials, on the school web site, such as inter-school competitions or staff training materials, etc.
- If pupils are editing images of pupils/staff, the supervising member of staff should take care to ensure that people are not misrepresented in an unfavourable or derogatory manner.

- Images which need to be accessed by pupils for a learning purpose must only be stored in a shared area on the school's network, for the length of the project. After this, the images must be deleted, or if the images are still required, they should be stored in a staff only area.
- It is recommended that staff collecting digital images should do so using cameras/digital devices owned by the school and delete them once saved into the school's files.

How published content is managed

- The contact details on the website and social media should be the school address, email and telephone number.
- Staff or pupils' personal information must not be published.
- The Head will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Written permission from Parents/Carers will be obtained before images/videos of pupils are electronically published.

Publishing pupils' images or work

- Images or videos that include pupils will be selected carefully.
- Written or verbal permission from parents or carers will be obtained before images/videos of pupils are electronically published if those images/videos identify individual pupils.
- The school reserves the right to publish images/videos showing groups of pupils without seeking permission where group images do not identify individual pupils by name.
- Pupils' work can only be published with their, or the parents' permission.

Management of social networking, social media and personal publishing

- Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.
- All staff should be alert to the potential risks of using social networking sites or personal publishing either professionally with pupils or personally. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.
- Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their Parents/Carers, particularly when concerning pupils' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour is outlined in the school Acceptable Use Policy (Appendix C).
- Communication on any device within school which can be interpreted as being material and/or links to extremist or terrorist groups will be reported immediately to the school's Network Manager and Designated Safeguarding Lead (see The Prevent Duty Policy).

Management of filtering

- It is important to recognise that filtering is not 100% effective. There are ways to bypass filters such as using proxy websites.
- Teachers should always evaluate any websites before using them with their pupils; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the school's Network Manager who will then escalate the concern as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk-assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- Any material that the school believes is illegal will be reported to appropriate agencies such as the Police or CEOP.

Management of Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with this policy

Protection of Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR which came into effect May 2018. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures

Information can only be kept about persons for specific school-related purposes. The information should be kept to a minimum and for as short a period as necessary. It should be removed when the purpose for its use is completed. Users should not have files of any type on any network servers, local hard disks or on the email system that contain information on a person that they would not like that

person to see. Any information that users do keep must be of a factual nature and not hearsay. Any person may, under the provisions of the Act, apply to see information about themselves in order to check the accuracy of the content. To delete such information after an application to view is received is an offence under the Act.

Users are obliged under the Act to take all reasonable steps to minimise unauthorised access to personal information stored on any school computer system. It must therefore be an offence to allow anyone else to
use your login name and password. Never leave any unattended computer logged on for more than a few minutes. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

Incidents of concern

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.)
- The Designated Safeguarding Leads will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the School Discipline and Pupil Behaviour Policy where appropriate.
- The school will inform Parents/Carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Greenwich Children's Services or the Local Authority designated officer and escalate the concern to the Police.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguarding Team to establish procedures for handling potentially illegal issues.

e–Safety complaints procedures

- Complaints about Internet misuse will be dealt with under the school's Complaints procedure.
- Any complaint about staff misuse will be referred to the Head of School.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.

Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the Internet, to deliberately hurt or upset someone" DCSF 2007
Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the School Discipline and Pupil Behaviour Policy (including Anti-Bullying Policy). There are clear procedures in place to support anyone in the school community affected by such bullying.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying.

In particular, section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents;
- gives Heads of School the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it is investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed, assistance from the police may be sought.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of cyberbullying.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. Pupils, staff and Parents/Carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
Sanctions for those involved in cyberbullying will be in line with the school's School Discipline and Pupil Behaviour Policy.

Mobile phones and personal devices

- Pupils are not permitted to bring a mobile phone to school at all. Mobile phones that are brought into school will be confiscated and returned at the end of the half term in which the phone was confiscated.
- The sending of abusive or inappropriate messages, content or trolling via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- If a mobile phone is confiscated, it might be searched by the Senior Leadership Team. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

Staff Use of Personal Devices

- It is recommended that staff do not use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. If they do, they should record this on the Home School contact form.
- Staff will be issued with a school phone where contact with pupils or Parents/Carers is required.
- Mobile phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching
  periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity, then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- It is recommended that staff collecting digital images should do so using cameras/digital devices owned by the school.
- If staff have images of pupils on their own digital devices, they must be transferred to the school's archive and then removed from their computers or digital storage devices.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Communication of the Policy

<u>With pupils</u>

- All users will be informed that network and Internet use will be monitored.
- Student instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.
- Appendix A, a summary of the e safety and Acceptable Use policy will be shared with the pupils, staff and Parents/Carers.

<u>With staff</u>

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement the e-Safety and Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All staff will read and sign Appendix C at the time of employment.

With Parents/Carers

- Parents/Carers attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- Parents/Carers and students will be requested to sign an e–Safety/Internet Agreement as part of the Home School Agreement at admission.
- Parents/Carers will be encouraged to read the e-Safety and Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for Parents/Carers on e–Safety will be made available to Parents/Carers in a variety of formats.
- The e-Safety and Acceptable Use Policy will be published on the school website.

With Governors

- The e-Safety and Acceptable Use policy will be published for all governors on the school website.
- The e-Safety and Acceptable Use Policy will be reviewed by governors annually.

Appendix A

Internet Agreement

All pupils and their Parents/Carers are asked to read and sign an agreement covering the expectations we have of pupils using the Internet in school.

Dear Parents/Carers

Responsible Use of the Internet

Pupils have access to the Internet at school. Mindful of the problems there are with children gaining access to undesirable materials, we have taken steps, along with the Local Authority, to deal with this.

Our Internet access has a built-in filtering system that restricts access to sites containing inappropriate content. All our screens are in public view and an adult is present.

No system is perfect however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material. We have been asked by the LA to inform you of the rules which the pupils are expected to follow to help with our precautions.

I would ask you to look through these rules and discuss them with your child and then return the signed form to us at school.

The e-Safety and acceptable use policy is enclosed.

Appendix B

St Thomas More Primary School Pupil Acceptable use agreement

This is to be read through with your parent/carer and then signed.

Use of the Internet

In order for pupils at St Thomas More to browse the Internet or make use of other technologies, we require each child (and their parent or carer) to sign to show that they understand the importance of adhering to these strict rules:

- *I will only use the Internet when I have permission and I am supervised*
- *I will not give out my address, home or mobile telephone number, photograph or school name and address on the Internet or in an email. I will not give out personal details of another child or adult either*
- *I will tell a teacher, parent or carer straightaway if a stranger tries to contact me on the Internet or by email*
- *I will tell my teacher straightaway if I come across any unsuitable pictures or information on the Internet by accident or if anything makes me feel uncomfortable or upset*
- *I will only use search engines or websites that have been chosen by a teacher. I will not try to access any inappropriate websites, chat rooms, Instant Messaging or Social Networking sites in school (Facebook/ Twitter etc.)*
- *I will not use social media to make negative comments about the school, its staff or other pupils*
- *I will not bring my mobile phone into school except in exceptional circumstances with the agreement of the Headteacher. The phone will then be stored in the office during the school day with the onus on the child to collect their phone.*
- *I will not download/upload any files from the Internet in school unless I have permission*

Pupil I understand the rules above and agree to follow them. If I break any of these rules, I understand that:

1. *Parents/carers may be contacted*
2. *I might be banned from using the Internet for a given period*
3. *More serious action might be taken*

Pupil Signature: _____ Date: ___/___/___

Parent/Carer I give permission for my child to use the Internet, email and other technologies in school. I understand that pupils will be held accountable for their own actions and agree to appropriate sanctions being imposed if rules are broken. I am aware that some materials on the Internet may be offensive and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.

Name of Pupil: _____

Parent/Carer Signature: _____ Date: ___/___/___

St Thomas More Primary School

Acceptable Internet Use Statement for Staff

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff and pupils requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to School Services.

- All internet activity should be appropriate to staff professional activity or the student's education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all email sent and for contacts made that may result in email being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Social networking sites. It is forbidden for a member of staff to contact a pupil or ex pupil under the age of 18, through a social networking site or via any other digital communication medium.
- iPads and other devices (those that are the property of the school) must be used appropriately in line with the e-Safety and Acceptable Use Policy at all times.

Signature _____

Name _____

Date _____

St Thomas More Primary School

Use of Digital Images Policy

Digital images whether still or moving can make an important contribution to the learning and teaching of our pupils. They also make an invaluable contribution to recording the life and activities of the school community. It is therefore important that during these processes staff and pupils avoid issues, which may prove to be areas of conflict, and potential catalysts for misconduct or offence.

- Digital images or video collected during school activities remain the property of the school.
- Pupils or staff cannot take a copy or transfer images to a portable storage device, or include them as an email attachment without permission of the Head of School.
- Staff or pupils taking images / recordings around the school should notify others of the purpose of their recording, before they capture the images.
- Images of staff or pupils should not be taken without their permission.
- Images which need to be accessed by pupils for a learning purpose must only be stored in a shared area on the school's network, for the length of the project. After this, the images must be deleted, or if the images are still required, they should be stored in a staff only area.
- It is recommended that staff collecting digital images should do so using cameras owned by the school.
- If staff have images of pupils on their own cameras / phones they must be transferred to the school's archive and then removed from their own computers or digital storage devices.
- Only images of staff or pupils who have given the requisite permission may have their images used on the school website, or in school publicity materials.

Signature _____

Name _____

Date _____