ST. THOMAS MORE HIGH SCHOOL
ACADEMY

E-Safety Policy

Approved by SLT:	**September 2024**
To be Reviewed and Approved:	**September 2025**

Mr Daniel Cauchi
Chair of the Governing Body

The School's Mission Statement

To inspire, To learn, To achieve,

To keep our Catholic ethos at the centre of our lives,

To fulfil our educational potential, welcoming all and reaching out to the wider world,

To truly be God's servant first.

E-SAFETY POLICY FOR ST THOMAS MORE HIGH SCHOOL

KEY CONTACTS WITHIN THE SCHOOL SEPTEMBER 2024

DESIGNATED SAFEGUARDING LEAD
NAME: MR GEOFF MASON : Member of SLT
CONTACT NUMBER: 01702 606771

DEPUTY SAFEGUARDING LEAD
NAME: MRS MICHELLE WALFORD
CONTACT NUMBER: 01702 606773

CHAIR OF GOVERNORS
NAME: DANIEL CAUCHI

NOMINATED GOVERNOR FOR SAFEGUARDING AND CHILD PROTECTION
NAME: LORRAINE MCCLEAN

DESIGNATED LEAD FOR LAC
NAME: MRS ALISON LINDSAY : Member of SLT
CONTACT NUMBER: 01702 606712

EMERGENCY OUT OF HOURS CONTACT FOR STAFF :
gmason@st-thomasmore.southend.sch.uk
mwalford@st-thomasmore.southend.sch.uk

DIRECT OUT OF OFFICE HOURS FOR C-SPOC
See number below for direct referral

KEY CONTACTS WITHIN THE DIOCESE OF BRENTWOOD

NAME: Mr Rob Simpson (Diocesan Director of Education)
CONTACT NUMBER: 01277 265284

KEY CONTACTS WITHIN THE LOCAL AUTHORITY

CSPOC **Children's Social Care,** **Southend City Council:** Where the school has concerns for the safety and welfare of a child or young person. **OUT OF OFFICE HOURS:** To make URGENT referrals	01702 215007 c-spoc@southend.gov.uk 0345 606 1212
SAFEGUARDING & CHILD PROTECTION CO-ORDINATOR and LOCAL AUTHORITY DESIGNATED OFFICER (LADO): Where there are concerns/allegations in respect of people working with children **SAFEGUARDING ADVISOR:**	ALLISON FRANCIS 01702 534539 allisonfrancis@southend.gov.uk SHARON LANGSTON 01702 534591 LADO@southend.gov.uk

E-Safety Policy

Contents

1. Introduction

E-Safety encompasses Internet technologies, communications using computers and other electronic devices such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate all members of the school community about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The responsibility for e-safety is not solely delegated to technical staff, or those with a responsibility for ICT but relates to all members of the school community including governors, staff, students, parents, volunteers, and visitors.

This policy should be read in conjunction with other policies including:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Health and Safety Policy
- Safer Recruitment Policy
- Whistleblowing Policy
- Allegations of Abuse against Staff Policy
- Sexual Violence, Sexual Harassment and Sexual Bullying Policy
- Assisi Catholic Trust Data Protection Policies

2. Purpose

The purpose of this policy is to ensure that all relevant members of the school community are educated in the legal, moral, prudent, and safe use of electronic and online communication and information technologies. This policy pays particular regard to the potential dangers that these technologies have in respect of matters such as bullying and child protection.

This policy also ensures that the schools' practices in respect of its use of these technologies guards the safety and security of its staff and students.

3. Responsibilities

The responsibility for maintaining safe and secure use of electronic and online technologies lies with everybody. However, specific responsibilities for the implementation of this policy, additional safeguarding measures, monitoring, reporting, and training are given to designated individuals.

3.1 Local Governing Committee

Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. A member of the Local Governing Committee is designated the role of Child Protection Governor and serves as the link Governor for e-safety.

3.2 Headteacher and Senior Leadership Team

The Headteacher has a duty of care for ensuring the safety (including e-safety) of all members of the school community, though the day-to-day responsibility for e-safety is delegated to the Assistant Headteacher - Attendance and Safeguarding who acts as the E-Safety Coordinator. It is the responsibility of the Headteacher and Senior Leadership Team to ensure that:

- The Designated Safeguarding Lead and all other relevant staff receive suitable training to enable them to carry out their e-safety roles.
- There is sufficient support and financial provision for the installation and implementation of technologies required to fulfil the needs of e-safety.

3.3 Assistant Headteacher - Attendance and Safeguarding

The Assistant Headteacher - Attendance and Safeguarding is the schools Designated Safeguarding Lead and has overall responsibility for e-safety and this e-safety policy.

The Assistant Headteacher - Attendance and Safeguarding will ensure, in liaison with others, that:

- The formal curriculum and extra-curricular programmes ensure that staff, students, and parents of the school are educated in the legal, moral, prudent, and safe use of 'electronic' and 'online' communication and information technologies and that these programmes are reviewed annually.
- Information, guidance, and training for parents in matters of e-safety, including school policies, take place each year and that parents receive updates throughout the year as necessary.
- Staff receive e-safety training.
- Staff receive training in how to deal with pastoral and disciplinary issues arising from electronic and online technologies.
- Protocols regarding the safe storage, use, communication and disposal of staff and student information and data to ensure their protection.
- Reviews of the schools e-safety policy and all relevant and related policies are undertaken annually and presented to the Senior Leadership Team with any recommendations for adjustment.
- The school obtains consent for the use of images and related information from students and parents.

3.4 IT Manager

The IT Manager is responsible for the correct and efficient operation of the schools own Information Communications Technologies and for ensuring, in liaison with others, that:

- The school's technical infrastructure is secure and not open to misuse or malicious attack as far as is practicable.
- The school meets required e-safety technical requirements and any relevant body e-safety guidance that may apply.
- The use of all aspects of the schools Information Communication Technologies is monitored and controlled in order that any misuse is mitigated or reported.

3.5 Staff

All staff are responsible for ensuring that all members of their school community are safe in all aspects of school life including during the use of electronic and online technologies. Staff should ensure that:

- They have an up-to-date awareness of e-safety and of the schools current e-safety policy and procedures and all other relevant polices.
- They have read, understood, and signed the ICT Usage & Code of Practice for Staff (Appendix B).
- They report any suspected misuse or e-safety issue to the Designated Safeguarding Lead or Pupil Support Team.
- They embed e-safety in all aspects of the curriculum and other school activities.
- Students understand and follow the ICT Usage & Code of Practice for Students (Appendix A).

3.6 Students

All students have a responsibility to ensure that they and their fellow students remain safe when using electronic and online technologies. Students should ensure that:

- They use the schools ICT systems in accordance with the ICT Usage & Code of Practice for Students (Appendix A).
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials.
- Understand the importance of adopting good e-safety practice when using electronic and online technologies in and outside of the school setting.

3.7 Parents

Parents and carers play a crucial role in ensuring that their children understand the need to use electronic and online technologies in an appropriate way. The school will take every opportunity to help parents understand these

issues through parents' evenings, newsletters and resources published on the school's website. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow other related guidelines.

4. Education and Training

Parents and carers play a crucial role in ensuring that their children understand the need to use electronic and online technologies in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters and resources published on the school's website. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow other related guidelines.

4.1 Educating Students

The school curriculum includes lessons, activities, and workshops in e-safety for all pupils with the intention to develop pupils' awareness, resilience, and skills in the wider electronic world. The school also supports parents and carers in their role in ensuring their children remain safe using electronic and online technologies. The school implements the following to educate and protect students:

- All year groups have a reminder lesson on E-Safety at the beginning of each academic year (See Computing curriculum plans).
- All new Year 7 students are taught and discuss the dangers of being on-line both whilst in school and at home. They are reminded of their responsibilities throughout their life at the school.
- All students in years 7-11 take part in an E-Safety lesson to mark E-Safety Day in February.
- Each new student is given a personal password and a talk on the need for it to remain confidential, and of his or her responsibility to keep it confidential.
- Each student is told who to report any problems or concerns to if they encounter problems or accidentally access inappropriate materials online.
- Each parent/student signs the section in the School Planner relating to school code of conduct and policies.
- Students are informed of the consequences of misusing information technology in school and the consequences of their misuse. This may include the download of pornographic images, and the appropriate use of mobile phones in school.
- Potentially damaging websites are filtered through the school computer network.
- The school promotes the use of anti-bullying and CEOP reporting facilities on the school website and Teams.
- Students access a wide range of e-safety topics in the school's Personal Development programme including topics on:
    - Risk of Sexting
    - Social media and digital relationships
    - Grooming
    - Recognising bias or misleading information online including AI manipulation
    - Digital literacy skills
- Guest speakers and workshops are invited in to talk and perform in assemblies at least once a year on E-Safety issues.
- The school participates in Anti-Bullying Week, which covers cyberbullying.

4.2 Educating Parents

The school is committed to helping parents and carers in their role in ensuring their children remain safe using electronic and online technologies. The school implements the following to educate and support parents:

- All parents have access to the school's website that allows them to read all school policies. These policies include the ICT Usage and Code of Practice for Students (Appendix A).
- E-Safety Information Evenings are organised at least once per academic year where parents are invited into school to learn about e-safety. Guest speakers are invited to speak about the potential risks.
- The school offers and undertakes online, level 1 certificate in E-Safety awareness for all parents that have requested it.

4.3 Training Staff

The school is committed to ensuring all staff are trained in E-Safety, Prevent and Safeguarding, no matter what their role is in the school to ensure students remain safe using electronic and online technologies. The school implements the following training for staff:

- E-Safety training is designed to inform all teaching and support staff of the dangers posed for students in their care in using all electronic and other communications and any other information technology use.
- E-Safety training is given as one part of the School's Child Protection training programme.
- Staff are made aware of their responsibilities in ensuring the students are protected by educating them in the legal, moral, prudent, and safe use of all electronic and online technologies.
- All staff undertake training in Online Safety.
- All staff are reminded that the E-Safety Policy is available in the policy area in Teams during the staff training days in September.
- All staff must read and acknowledge doing so by email acceptance.
- All new staff to the school are made aware of the E-Safety policy, its requirements, implications, and their responsibilities as part of the school's new staff induction training on Child Protection.
- Key members of staff have attended e-safety workshops run by the Local Authority and have cascaded information to the relevant groups responsible for e-safety in school. This includes The Assistant Headteacher - Attendance and Safeguarding, the Director of Finance and Operations, the IT Manager, the Pupil and Community Support Officer and members of the ICT department.
- The Head of Computing & Head of Computer Science co-ordinate departmental training on e-safety and ensures all members of the Computing department are fully aware of their responsibilities.
- The Computing Scheme of Work includes e-safety training for students and the Head of Department therefore ensures all members of the department are fully conversant with the expectations to better e-safety within the curriculum.
- Staff training on e-safety is part of the schools wider training programme on Child Protection and is regularly reviewed by the Senior Leadership Team and ICT departments.
- The IT Manager and Director of Finance and Operations will ensure that the relevant staff are informed of any changes to the school's ICT System and therefore new training requirements.

5. Audit

#	5.1 Policies and Practices	Supporting Evidence
1.	Does your organisation have an e-safety policy?	Yes
2.	Who is responsible for co-ordinating e-safety in your organisation to ensure that best practice is developed, implemented, and kept up to date?	Mr Geoff Mason (Assistant Headteacher - Attendance and Safeguarding.).
3.	Is there a regular risk assessment of your e-safety infrastructure? If so, how often?	An E-Safety audit is undertaken annually.
4.	Do all your services have acceptable use polices for students, staff, and parents?	See Appendices of E-Safety Policy: ICT Usage and Code of Practice for Staff (Appendix B) ICT Usage and Code of Practice for Students (Appendix A) ICT Usage and Code of Practice for IT Administrators (Appendix D)
5.	Is the application of these policies monitored?	Yes
6.	Are the acceptable use policies kept up to date in line with changing issues and technologies?	Policies are reviewed annually in line with the E-Safety Policy review.
7.	Are the students that use your services aware of their responsibilities for staying safe when online? (e.g., keeping passwords confidential, not sharing confidential or person identifiable information)	Students are given guidance when they enter the school in Year 7 and reminded throughout their time at school in e-safety workshops and activities.
8.	Do students using your service know who to speak to if they encounter problems online or accidentally access inappropriate materials?	Staff inform students as to the procedure to report problems. There is an anti-bullying and CEOP button on the school website that students can use to submit a report online.
9.	Is personal data collected, stored, and used according to the principles of the General Data Protection Regulation?	The ICT Usage and Code of Practice for Students and Staff refers to the General Data Protection Regulation.
10.	Does your service obtain consent for use of images and related information from child/young person and/or person with parental responsibility for the child?	Parent's consent on the Pupil Data Form.
11.	What are the procedures for reporting e-safety incidents of misuse?	See School Student Behaviour Policy and Code of Conduct in Student Planner.
12.	Are staff aware of their responsibilities in responding to certain types of incidents?	See School Student Behaviour Policy and Code of Conduct in Student Planner.

#	5.1 Policies and Practices	Supporting Evidence
13.	How are incidents escalated?	See School Student Behaviour Policy and Code of Conduct in Student Planner.

#	5.2 Infrastructure and Technology	Supporting Evidence
14.	Does your organisation have filtering systems in place to prevent access to inappropriate material?	Smoothwall Web Filter is installed and administered on-site.
15.	Are you using accredited Internet Service Providers (ISPs)?	Southend City Council E2BN.
16.	Does your Acceptable Use Policy (AUP) make it clear who can send/receive external email, the type of language used, and type of attachments sent/received?	See Policy appendices ICT Usage and Code of Practice for Staff and Students.
17.	Does everyone (staff and students) have their own username and private password that they use to log onto the internet and email?	Yes
18.	Do you have anti-virus and anti-spam systems in place and are they updated regularly?	Sophos Central / Sophos Intercept-X / Smoothwall Unified Threat Management Gateway.
19.	Do you allow mobile devices to connect to your network and is their use covered in your Acceptable Use Policy (AUP)?	BYOD network only. Unencrypted removable storage devices are permitted only for students. BitLocker encryption is enforced for all staff removable storage devices.
20.	If your network uses wireless, is this a secure encrypted service?	Wireless network is secured using WPA2 encryption.
21.	Do you monitor ICT systems including the use of internet and email?	Teachers in ICT rooms have monitoring facilities. Automated alerts are sent to the Pupil Support Team if access to online material deemed inappropriate (inc. Prevent) is attempted. The school operates a formal Email Approval Process for students (Appendix J).
22.	Is there a process in place for dealing with incidents?	Student: Behaviour Policy and Staff: Discipline Policy

#	5.3 Communication and Training	Supporting Evidence
23.	How does your organisation seek to raise awareness about the safe use of the internet and other technologies? a) with students b) with staff c) with parents	See ‘Education and Training’ section of the E-Safety Policy.

#	5.3 Communication and Training	Supporting Evidence
24.	Are you aware of CEOP? (Child Exploitation & Online Protection Centre http://www.ceop.gov.uk) If so, do you access development and delivery of training and education programmes with CEOP?	Resources have been accessed and used in training. Links to CEOP are available to everyone via the school website homepage.
25.	Does your organisation have a strategy for educating and training staff in e-safety? If so, how many of your staff have received: • Induction training • Ongoing support/training	The school has undertaken online E-Safety and Prevent training for all staff that is ongoing and renewed annually. Staff undertake NCSC Cyber Security Awareness training annually.
26.	Are there additional safeguards in place for children with additional vulnerabilities? If so, please specify what these additional safeguards are.	SEN students will often have LSAs monitoring their work. Staff will be alerted of those over whom there are pastoral concerns.
27.	How will the impact of education and training be monitored and evaluated?	Incidents related to E-Safety are recorded by the Pupil Support Team and reported in monthly SLT Data.
28.	What e-safety information and guidance is provided to parents and carers?	Parents are aware of the AUP that their sons/daughters are required to sign. • There are information evenings for parents. • The school offers Online Safety training to parents.

#	5.4 Standards and Inspection	Supporting Evidence
29.	Is there a designated lead for monitoring E-Safety measures within your organisation?	The Lead Professional in the School for 'E-Safety' is the Assistant Headteacher - Attendance and Safeguarding. See the 'Responsibilities' section of the E-Safety Policy.
30.	How is email and online activity monitoring co-ordinated, particularly where several organisations are using your facilities?	External organisations using our system are given an individual user account.
31.	Are emerging themes and trends passed to a central coordinator within your organisation?	The IT Manager records any difficulties with the system including any breaches of E-Safety that are passed, when appropriate, to the Pupil Support Team or Designated Safeguarding Lead.
32.	How are safety mechanisms measured, and how is progress benchmarked?	a) Hardware and software safety-mechanisms are measured by their success. If they are not adequate, they are replaced. b) Student education is measured by the number of incidents. c) Staff training is not yet formally evaluated though any malpractice is reported and recorded.

#	5.4 Standards and Inspection	Supporting Evidence
33.	How is good practice shared?	Good practice is shared in a number of ways depending upon the point at hand. A variety of mechanisms are available to us, e.g.: Staff briefings, lessons, assemblies training days.
34.	How is poor performance managed?	a) Poor performance by students is managed through the pastoral and discipline procedures. b) Poor performance by staff is managed through the Performance Management Policy, Capability Policy, and Disciplinary Policy.
35.	Who drives forward recommendations?	Recommendations will be driven forward by several staff, e.g.: Senior Leadership Team, Pupil Support Team members, ICT Staff, IT Support Team.

6. Revision and Review History

Version 2.0	23rd November 2017	Draft
Version 2.1	30th November 2017	Initial Version
Version 2.2	22nd May 2018	Policy Review Updated section to reference GDPR (5.9). Updated all appendices.
Version 2.3	26th November 2018	Removed reference to 'Safer use of Images Policy', a separate document that is now included as 'Appendix E' in the E-Safety Policy. Updated Appendix E Safe Use of Images Guidance Policy and references to the "Use your camera courteously" code.
Version 2.4	23rd October 2019	Policy Review Updated Appendix F Use of Mobile Phones and Social Media Guidance Policy.
Version 2.5	26th June 2020	Policy Review Updated Appendix A ICT Usage and Code of Practice for Students Updated Appendix B ICT Usage and Code of Practice for Staff
Version 2.6	6th September 2021	Policy Review Updated 4.2 and 4.3 references to VLE no longer relevant. Updated audit inc. references to new AV/Threat management software and CEOP resources. Updated references to new location of CEOP resources throughout.
Version 2.7	20th October 2021	Updated Appendix D to replace CCTV Policy with CCTV Procedure.
Version 2.8	16th December 2021	Reordered appendices. Added two further documents as appendices: Privileged User Accounts Policy ICT Usage and Code of Practice for IT Administrators
Version 2.9	27th October 2022	Policy Review Updated 3.1 Local Governing Body to reference 'Local Governing Committee' not 'Governing Body'. Updated 5 Audit, Section 4 to include reference to individualised Acceptable Use and Code of Practise documents including the 'ICT Usage and Code of Practice for IT Administrators'. Updated 5 Audit, Section 14 to remove reference to legacy SBC filtering system no longer in use. Updated 5 Audit, Section 19 to remove 'Guest' Wireless Network no longer used. Updated details relating to encryption of staff removeable storage devices. Updated 4.1 Educating Students to reference new CPSHE curriculum and outlined modules that specifically cover E-Safety topics.
Version 2.10.2	8th September 2023	Policy Review Updated contents to reference new appendix and removed page numbers of appendices. Updated 4 Education and Training references to CPSHE and Personal Development provision and listed topics

		studied. Updated responsibilities of Head of ICT to Head of Computing and Head of Computer Science. Updated 5 Audit references to Director of Learning i/c Behaviour and Safety to Director of Behaviour and Safeguarding. Updated 5, Section 25 Audit to include reference to NCSC Cyber Security Awareness training. Updated Appendix F. See separate appendix F revision and review history for changes. Added Appendix I: Filtering and Monitoring Policy in line with new DfE 'Meeting digital and technology standards in schools and colleges' guidance.
Version 2.11	23rd September 2024	Policy Review Updated contents to reflect changes below. Updated Section 1 to include reference to the Assisi Catholic Trust Data Protection Policies. Updated Section 3.2 Headteacher and Senior Leadership Team referenced to Director of Behaviour and Safeguarding updated to Assistant Headteacher - Attendance and Safeguarding. Updated Section 3.3 Director of Behaviour and Safeguarding references to Director of Behaviour and Safeguarding updated to Assistant Headteacher - Attendance and Safeguarding. Updated section 4.1 Educating Students to reference AI manipulation. Updated section 4.3 Training Staff references to Director of Behaviour and Safeguarding updated to Assistant Headteacher - Attendance and Safeguarding. Updated reference to 'Level 1 E-Safety Training' to 'Online Safety' training. Updated 5 Audit, Section 2 to include correct position. Updated 5 Audit, Section 21 to include new student Email Approval Process. Updated 5 Audit, Section 28 to reference 'Online Safety' training for parents. Added Appendix J Email Approval Process Flowchart Updated Appendices See individual appendix revision and review history for associated changes.

Appendices

Appendix A: ICT Usage and Code of Practice for Students
Appendix B: ICT Usage and Code of Practice for Staff
Appendix C: Privileged User Accounts Policy
Appendix D: ICT Usage and Code of Practice for IT Administrators
Appendix E: School Gateway Usage Policy
Appendix F: CCTV Code of Practice and Usage Policy
Appendix G: Safe Use of Images Guidance Policy
Appendix H: Use of Mobile Phones and Social Media Guidance Policy
Appendix I: Filtering and Monitoring Policy
Appendix J: Email Approval Process Flowchart

Appendix A

St Thomas More High School

ICT Usage & Code of Practice for Students

Introduction

The ICT System is owned by the school and may be used by students to further their education. The ICT Usage & Code of Practice for Students has been drawn up to protect all parties including students, staff, parents, guardians, and the school. The school reserves the right to monitor all Internet access including access made via personal devices when connected to the school network. The school reserves the right to monitor internet access examine or delete any files that may be accessed or held on its ICT System.

All students must sign a copy of this ICT Usage & Code of Practice.

1. **Acceptable use of the ICT System**
   The following constitutes acceptable use of the school's ICT System by an individual.

   1.1 Students must keep all account passwords secure.
   1.2 Students must refrain from deleting system files, applications, or other students' work, or modify system or workstation settings.
   1.3 Students must refrain from attempting to gain access to unauthorised areas of the network or another user's documents area.
   1.4 Students must not knowingly transfer malicious software to the network.
   1.5 Students must not attempt to damage the ICT systems, including hardware and software.
   1.6 Students must not attempt to install any software, applications, or device drivers onto any school computer.

2. **Acceptable use of the Internet, email, and virtual learning platforms (VLP)**
   All Internet activity should be appropriate to the student's education. The following constitutes acceptable use of the Internet, email and all school provided access to virtual learning platforms by an individual.

   2.1 Students must respect copyright of material.
   2.2 Students must not undertake any Internet activity not appropriate to the school's aims and Catholic ethos.
   2.3 Students must not undertake activity that threatens the integrity of the school ICT system or that may attack or corrupt other systems.
   2.4 Students must not undertake activities for personal financial gain, gambling, political purposes, or advertising.
   2.5 Students must not undertake activities that access inappropriate materials, such as pornographic, racist, or offensive material.
   2.6 Students must report inadvertent access to inappropriate websites immediately to their teacher or available member of staff.
   2.7 Students must access email and any VLP only via an authorised account and password.
   2.8 Students must apply the same high standard of language and content to email as you would for letters or other public communication.
   2.9 Students must not attempt to bypass the schools Internet filtering by means of alternative or unauthorised software including Internet browsers or web based anonymous proxies.
   2.10 Students must refrain from downloading games or executable files not associated to their learning.
   2.11 Students accept that all Internet access made using a school provided device, including that which is encrypted, is subject to inspection by the school's web filtering systems.

3. Acceptable use of social media networking sites

The following constitutes acceptable use of social media networking sites by students.

3.1 Students must not access personal social media networking accounts using a school provided device.
3.2 Students must not use their personal equipment to access social media networking sites in school.
3.3 Only students with school authorisation to access specific social media networking sites may do so.
3.4 Inappropriate use of social networking sites that brings the schools catholic ethos and good name into disrepute, either within the school, or privately, could lead to disciplinary action.

4. Acceptable use of the wireless network

The following constitutes acceptable use of the school's wireless network by an individual using a personal device.

4.1 Students must only connect personal wireless enabled devices to the designated student wireless network.
4.2 Students must not attempt to gain access to any other school wireless network.
4.3 Students must not attempt to gain access to a school wireless network using any account other than their own.
4.4 Students accept that all Internet access made using a personal device, including that which is encrypted, is subject to inspection by the school's web filtering and threat management systems.

5. Acceptable use of a school provided laptop

Laptops are provided to students to support their learning. No other person is authorised to use a school provided laptop including parents, guardians, family, or friends. Students must return a school provided laptop to the school upon request.

6. Maintenance of a school provided laptop

Maintenance tasks will be undertaken by the IT Support Team. This includes system updates and upgrades to software applications to ensure the school complies with licensing agreements.

6.1 Students must not remove, reinstall, modify, or upgrade the operating system.
6.2 Students must not partition or format the laptop storage drive.
6.3 Students must report any error messages to the IT Support Team.

7. Security of a school provided laptop

Students are advised to make every reasonable attempt to keep the laptop safe and avoid damage.

7.1 Students must lock the laptop away, out of sight when it is left unattended, both in and out of school.
7.2 Students must use the laptop in the UK only. Should a pupil wish to use a laptop outside of the UK, permission must be sought from the Headteacher.

8. Insurance covering a school provided laptop

The school's insurance policy covers theft or attempted theft by forcible or violent means whilst the laptop is at the students' place of residence. The school's insurance policy states that insurers will not be liable for theft or attempted theft from a car unless the laptop is stored out of sight in a locked boot, with all doors, windows, and other openings securely locked and properly fastened and entry to the vehicle has been gained by forcible and violent means.

9. General care of a school provided laptop

The following guidelines are given to help ensure a laptop provides several years of service.

9.1 Students should not leave the laptop in extremes of temperature.
9.2 Students should not move the laptop from a cold environment to a warm environment and start the laptop up immediately.
9.3 Students should not clean the laptop with chemicals or abrasive cloths/brushes.
9.4 Students should not consume food or drink around the laptop.
9.5 Students should store the laptop in a cool, dry environment in a safe and secure place.
9.6 Students should ensure there is nothing on the keyboard when the lid of the laptop is closed.
9.7 Students should regularly run the laptop battery until it is fully discharged.

10. Revision History

Version 1.0	9th January 2014	Draft
Version 1.1	19th March 2014	Initial Version
Version 1.2	12th July 2013	Policy Update
Version 1.3	18th March 2016	Policy Review
Version 1.4	22nd May 2018	Policy Review Addition of revision history (10).
Version 1.5	26th June 2020	Policy Review Addition of parents and guardians to introduction (1). Virtual Learning Environment changed to Virtual Learning Platforms (2). Reference to who can use a school provided laptop added (5). Headings changed to reference provided laptops (5, 6, 7, 8, and 9).
Version 1.6	6th September 2021	Policy Review. No Changes.
Version 1.7	27th October 2022	Policy Review. Minor grammatical changes.
Version 1.8	8th September 2023	Policy Review. No Changes.
Version 1.9	24th September 2024	Policy Review. Section 1.5 updated to elaborate on what is included in 'ICT Systems'. Section 2.10 updated to elaborate on 'downloading games'. Section 6 references to ICT Technical Team updated to IT Support Team. Section 6.2 updated terminology to 'Storage drive'. Section 7.2 updated to permission from Headteacher.

Appendix B

St Thomas More High School

ICT Usage & Code of Practice for Staff

Introduction

This usage and code of practice policy aims to advise staff on the most effective way to use the school's ICT System in an efficient and safe manner. This guidance aims to protect all parties including the pupils, staff, and the school. By its very nature, the document does give advice on activities that individuals should avoid but this is not intended to restrict lawful and ethical activity. The use of the ICT System must conform to relevant legislation including the General Data Protection Regulation, Copyright, Designs and Patents Acts and the CCTV Code of Practice. The use of the school ICT equipment must be conducted in accordance with the Catholic ethos of the school.

The ICT System, including laptops, are the property of the school and should be used by staff to enhance their professional activities including teaching, research, administration, and management. Staff may use the ICT equipment for both professional and personal purposes, provided it is in accordance with the school's ethos.

All staff must sign a copy of this ICT Usage & Code of Practice.

1. **General Data Protection Regulation**
   St Thomas More High School will comply with the six principles contained in the General Data Protection Regulation, any associated legislation, and any future changes of legislation. The principles are:
   - Personal data shall be processed lawfully, fairly, and transparently.
   - Personal data shall be collected only for the specific legitimate purposes.
   - Personal data shall be adequate, relevant, and limited to what is necessary.
   - Personal data shall be accurate and kept up to date.
   - Personal data shall be stored only as long as is necessary.
   - Personal data shall be stored with appropriate security, integrity, and confidentiality.

2. **Digital Data Security**
   To conform with the seventh principle of the General Data Protection Regulation the following constitutes acceptable storage of sensitive or personal data by an individual.

   2.1 Staff must not remove, transfer, upload or copy sensitive or personal data from the school network to any unencrypted removable storage device.
   2.2 Staff must not use any email account other than that provided by the school to remove, transfer, upload, copy or send sensitive or personal data from the school network via email.
   2.3 Staff must ensure that any personal digital device that has access to a work provided email account must be kept secure at all times and secured with a password or PIN code when not in use.
   2.4 Staff must not remove, transfer, upload or copy sensitive or personal data from the school network to Internet based websites including social media sites.
   2.5 Staff must not store images or video of pupils on any personal digital device including digital cameras, mobile phones, smart phones and PDAs.
   2.6 Staff must not remove, transfer, upload or copy sensitive or personal data from the school network to any personal cloud-based storage service.

3. **Acceptable use of the ICT System**
   The following constitutes acceptable use of the school's ICT System by an individual.

3.1 Staff must agree that the school may examine or delete any files that are held on its ICT System.
3.2 Staff must agree that the school may monitor Internet activity and any emails sent and received.
3.3 Staff must report any inappropriate material found on the school network or misuse of the school's ICT systems by either staff or pupils to the Headteacher or his/her deputy.
3.4 Staff must log off or lock workstations left unattended to ensure the integrity and security of data held on the network.
3.5 Staff must keep all account passwords secure.
3.6 Staff must refrain from deleting system files, applications or other staff or pupils' work, or modify system or workstation settings.
3.7 Staff must refrain from attempting to gain access to unauthorised areas of the network or another user's documents area.
3.8 Staff must not knowingly transfer malicious software to the network.
3.9 Staff must refrain from downloading games or executable files. The IT Manager will assist staff who require subject specific executable files as part of their professional activity.
3.10 Staff must not attempt to damage the ICT systems, as this will be treated as a disciplinary offence.
3.11 Staff must not allow pupils to access the computer network using a staff username and password.
3.12 Staff must delete sensitive or personal data when it is no longer required.

4. Acceptable use of the Internet, email, and Virtual Learning Platforms (VLP)

Due to continuing advances in technology, it is not possible to guarantee safety when using the Internet. However, by working within the guidance given below, the risks can be reduced, and the school and its staff and pupils can be protected.

The following constitutes acceptable use of the Internet, email, and virtual learning platforms by an individual.

4.1 Staff must respect copyright of material.
4.2 Staff must not undertake any Internet activity not appropriate to the school's aims and Catholic ethos.
4.3 Staff must not undertake activity that threatens the integrity of the school ICT System or that may attack or corrupt other systems.
4.4 Staff must not undertake activities for personal financial gain, gambling, political purposes, or advertising.
4.5 Staff must not undertake activities that access inappropriate materials, such as pornographic, racist, or offensive material.
4.6 Staff must report inadvertent access to inappropriate websites immediately to the Headteacher or his/her deputy.
4.7 Staff must access email and any VLP only via an authorised account and password.
4.8 Staff must apply the same high standard of language and content to email as you would for letters or other public communication.
4.9 Staff are responsible for any email sent or content published on a VLP or any other public website.
4.10 Staff must not post anonymous messages or forward chain letters.
4.11 Staff must use a school email address for all school related electronic communication. Personal email must be sent, and received, using a separate, private email account.
4.12 Staff must not use peer-to-peer file sharing software. This is strictly prohibited.

5. Acceptable use of social media networking sites

The following constitutes acceptable use of social media networking sites by staff.

5.1 Staff must not access personal social media networking accounts using a school provided device.
5.2 Staff must not use their personal equipment to access social media networking sites in the school whilst in the vicinity of students when in public areas including classrooms, corridors other public areas and whilst on duty.
5.3 Staff may use their personal equipment to access social media networking sites in the school away from the vicinity of students when in private areas including the staff room and offices.
5.4 Only staff with school authorisation to access specific social media networking sites may do so.
5.5 Inappropriate use of social networking sites that brings the schools catholic ethos and good name into disrepute, either within the school, or privately, could lead to disciplinary action.
5.6 It is prohibited to 'friend' any student on roll on any social media networking sites unless authorised by the school.

6. Acceptable use of the wireless network

The following constitutes acceptable use of the school's wireless network by an individual using a personal device.

6.1 Staff must only connect personal wireless enabled devices to the designated staff wireless network.
6.2 Staff must not attempt to gain access to any other school wireless network.
6.3 Staff must not attempt to gain access to a school wireless network using any account other than their own.
6.4 Staff accept that all Internet access made using a personal device, including that which is encrypted, is subject to inspection by the school's web filtering and threat management systems.

7. Acceptable use of a school laptop

Laptops are for the use of staff to support their professional and personal activities. Staff must not allow anyone other than the IT Support Team to use a work laptop. Use by students, family or friends is prohibited. Staff must return a school provided laptop to the school upon request.

7.1 Staff must have the laptop available for use in school every day.
7.2 Staff must save work created for school use in the 'Documents' area of the laptop. Personal files must be stored on the local storage drive and are not backed up to the cloud. The member of staff takes full responsibility for making backup files of any personal data.
7.3 Staff must connect the laptop to the network for the duration of each lesson.
7.4 Staff must log off from the network when the laptop is not in use.
7.5 Staff must not install unapproved or unlicensed software onto the laptop. A licence for any software that is installed must be given to the IT Manager.
7.6 Staff must return the laptop to the school upon request.
7.7 Staff must ensure that in the event of leaving employment at the school, the laptop is returned to the school prior to the last working day.

8. Maintenance of a school laptop

Maintenance tasks will be undertaken by the IT Support Team. This includes system updates and upgrades to software applications to ensure the school complies with licensing agreements.

8.1 Staff must not remove, reinstall, modify, or upgrade the operating system. Updates and service packs should only be installed by the IT Support Team.
8.2 Staff must not partition or format the laptop storage drive.
8.3 Staff must not remove, reinstall, modify, or upgrade any software that is installed when the laptop is first issued. All software upgrades must be carried out by the IT Support Team.
8.4 Staff must report any error messages to the IT Support Team.

9. Security of a school laptop

Staff are advised to make every reasonable attempt to keep the laptop safe and avoid damage.

9.1 Staff must not remove, modify, upgrade, or disable the antivirus software.
9.2 Staff must not install any additional antivirus or firewall software.
9.3 Staff must not remove, modify, upgrade, or disable the encryption software.
9.4 Staff must not remove, modify, or alter any encryption configuration settings.
9.5 Staff must lock the laptop away, out of sight when it is left unattended, both in and out of school.
9.6 Staff must use the laptop in the UK only. Should a member of staff wish to use a laptop outside of the UK, permission must be sought from the Director of Finance and Operations.

10. Insurance covering a school laptop

The school's insurance policy covers theft/attempted theft by forcible or violent means whilst the laptop is at the staff member's place of residence. The school's insurance policy states that insurers will not be liable for theft/attempted theft from a car unless the laptop is stored out of sight in a locked boot, with all doors, windows, and other openings securely locked and properly fastened and entry to the vehicle has been gained by forcible and violent means.

11. General care of a school laptop

The following guidelines are given to help ensure a laptop provides several years of service.

11.1 Staff should not leave the laptop in extremes of temperature.
11.2 Staff should not move the laptop from a cold environment to a warm environment and start the laptop up immediately.
11.3 Staff should not clean the laptop with chemicals or abrasive cloths/brushes.
11.4 Staff should avoid consuming food or drink around the laptop.
11.5 Staff should store the laptop in a cool, dry environment in a safe and secure place.
11.6 Staff should ensure there is nothing on the keyboard when the lid of the laptop is closed.
11.7 Staff should regularly run the laptop battery until it is fully discharged.

11. Revision History

Version 1.0	20th January 2013	Draft
Version 1.1	29th January 2013	Initial Version
Version 1.2.1	12th July 2013	Policy Update
Version 1.2.2	19th May 2015	Policy Review
Version 1.3	18th March 2016	Policy Review
Version 1.4	22nd May 2018	Policy Review Revision of Data Protection Guidance in line with new legislation (1). Update to digital data security to reference GDPR (2). Addition of revision history (12).
Version 1.5	23rd October 2019	Policy Review
Version 1.6	26th June 2020	Virtual Learning Environment changed to Virtual Learning Platforms (2). Addition of request to return laptop to school added (7). Headings standardised (7, 8, 9, 10 and 11).
Version 1.7	6th September 2021	Policy Review. No Changes.
Version 1.8	27th October 2022	Policy Review. No Changes.
Version 1.9	8th September 2023	Policy Review. No Changes.
Version 1.10	24th September 2024	Policy Review. Section 7 and 8 references to ICT Technical Team updated to IT Support Team. Section 7.2 terminology updated to ‘Storage drive’ and ‘the Cloud’. Section 7.3 removed. No longer relevant. Section 8.2 terminology updated to ‘Storage drive’.

Appendix C

Assisi Catholic Trust

Privileged User Accounts Policy

Introduction

Network and systems administrators have privileges and duties that may bring them into contact with sensitive, restricted, or personal information during the course of their work. The purpose of this document is to ensure that administration roles and responsibilities are properly understood and that privileged accounts are used appropriately.

These guidelines apply to all personnel, including those providing services under contract, who are provided with Administrator or Privileged Access to school computing and information resources. This includes hardware systems and software applications.

1. **Definitions**
   Anyone with access that enables them to affect change that would be felt beyond their immediate job role could be considered a privileged user. For example, administering systems or networks which are critical to a business (e.g., database admins) or accessing systems used to perform a critical function (e.g., approving financial payments). Privileged Access is therefore defined as a level of access above that of a 'normal' user.

2. **Examples of users with privileged access:**
   - A School Business Manager account with the ability to process payments.
   - An external IT Support Technician account providing access to a server.
   - A DSL account with read/write access to a safeguarding reporting application.
   - A curriculum subject leader account with access to add/remove users from a curriculum app.

3. **Types of Administrative Accounts**

   - **Local Administrative Accounts**
     Non-personal accounts that provide administrative access to the local host or instance only.
     Example: Staff member who has been given an admin account to make changes, add users, or perform maintenance on a specific workstation or laptop.

   - **Application Administrative Accounts**
     Accounts used by applications to access databases, external third-party applications, or services.
     These privileged accounts usually have broad access to underlying company information that resides in applications and databases.
     Example: Administration staff with write access to the schools Management Information System (MIS).

   - **Domain Administrative Accounts**
     Privileged administrative access across all workstations and servers in one, or more than one, domain.
     These accounts provide the most extensive access and any compromise to the security of this type of account is serious and puts the school at risk.
     Example: IT personnel that monitor connectivity and implement group policy across the whole network.

   - **Emergency Accounts**
     Unprivileged users with administrative access to secure systems in the case of an emergency and are

sometimes referred to as 'break glass' accounts. It is recommended that there are at least two users with privileged access for any system. This reduces the need to make sudden decisions in an emergency.
Example: Staff illness prevents admin access, and the school can't provision new accounts or make system modifications. A new admin account is needed to maintain functionality and core business functions.

4. Privileged User Accounts

Privileged user accounts have specific additional access to one or more systems or applications.

- Accounts must have unique and complex passwords.
- Monitoring of account use should be undertaken, and access should be periodically reviewed.
- Documentation should be undertaken when staff are granted enhanced access to systems.

User accounts should always follow the 'least privilege' principle. Users should only be provided with accounts with sufficient access for the requirements of their role.

Staff should have separate user accounts if they are expected to perform both administrative and routine functions.

Administrators should log in with standard user accounts for day-to-day tasks.

Privileged user accounts must be approved by the Headteacher (or their deputy) or Chief Financial Officer (or their deputy) in liaison with the Trust IT Manager (or their deputy).

5. Data Integrity

Administrators must ensure their activities do not result in the loss or destruction of information.
If a change is made to stored data, then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

6. Monitoring

Administrators must not act to monitor or enforce policy unless they are sure that all reasonable efforts have been made to inform users that both such monitoring will be carried out, and the policies to which it will apply.

If this has not been done through a general notice to all users (such as the ICT Usage & Code of Practice for staff) then individual permission must be obtained from file owner(s) before a file is examined. If a network communication is monitored, all parties should provide consent before monitoring takes place.

7. Appropriate Use of Administrator Access

Privileges provided to administrators are solely for the purposes of supporting the smooth running of the school and to enable the school to ensure maximum availability, data integrity and security for the systems they are responsible for.

The use of Administrator Access should be consistent with an individual's role or job responsibilities as prescribed and authorised by the Strategic Leadership Team. When an individual's role or job responsibilities change, Administrator Access must be reviewed and appropriately updated or removed.

In situations where it is unclear whether a particular action is appropriate, and within the scope of current job responsibilities, the situation should be discussed with the Headteacher or Chief Financial Officer.

8. Reporting Requirements

Report any suspected violation of the schools E-Safety Policy to the Headteacher or Chief Financial Officer. This includes suspected inappropriate use of Administrator Access.

Report any data or security breach concerns to the Headteacher or Trust IT Manager promptly, providing information as to the date, time, location, and potential extent of any breach.

9. Exceptions

Requests for exceptions to any information security policies may be granted for documented and explicit reasons with compensating controls in place to mitigate risk.

10. Privileged access review

The following will trigger an automatic review of access and consideration for revocation:

- Notice to leave a post.
- A change of role.
- Contractual expiry.
- Breach of policy or user actions which may lead to disciplinary action.

11. Appendix

11.1 Appendix D - ICT Usage and Code of Practice for IT Administrators

12. Revision History

Version 1.0	11th November 2021	Draft
Version 1.1	16th December 2021	Initial Release
Version 1.2	27th October 2022	Policy Review. No Changes.
Version 1.3	8th September 2023	Policy Review. No Changes.
Version 1.4	24th September 2024	Policy Review. Policy rebranded to the Assisi Catholic Trust. Logo and organisation name changed to cover all schools in the Trust. References to IT Manager and Director of Finance and Operations updated to Trust IT Manager and Chief Financial Officer.

Appendix D

ICT Usage and Code of Practice for IT Administrators

System administrators must:

1. Restrict the use of accounts with privileged access to functions consistent with the administrator's role, job responsibilities, and the purpose for which the access was granted.
2. Ensure that networks, systems, and services are available to authorised users only.
3. Ensure information is handled and transferred correctly, preserving its integrity, and providing an appropriate level of security for the classification of the data being processed.
4. Ensure that default passwords are changed using strong password methodologies when an Information System is installed or implemented.
5. Where necessary, monitor compliance with IT policies which apply to the systems being administrated and act in support of school policies at all times.
6. Monitor and record network traffic if defined as being in the scope of the role.
7. Take steps to ensure adherence to, and compliance with, all hardware and software license agreements entered into and communicated by the school.
8. Examine relevant files as part of necessary security investigation if defined as being in the scope of the role.

In addition to activities deemed inappropriate in the school's ICT Usage & Code of Practice for Staff, IT Administrator's must not:

1. Bypass user access controls or any other formal security controls, without approval.
2. Bypass formal account activation, suspension or change procedures, including enhancing user permissions without authorisation.
3. Bypass security measures or access restrictions applied to protect information or access to information that is outside the scope of specific job responsibilities.
4. Disclose information, accessed as part of authorised works, to those unauthorised to view it.
5. Use additional access to satisfy personal curiosity about an individual, system or school practice.
6. Monitor user activity which is not authorised and/or does not form part of routine monitoring encompassed by school policy.
7. Use administrative accounts when there is not a business need to do so.
8. Attempt to make readable the content of a file or communication that appears to have been deliberately protected by the owner, for example by encrypting it, without specific authorisation from management or the owner of the file.
9. Use administrative credentials to access systems with untrusted devices.

I have read the guidelines for Privileged IT Accounts and agree to abide by the ICT Usage & Code of Practice for IT Administrators.

Name: _____ **Job Role:** _____

Signature: _____ **Date:** _____

Authorised by: _____ **Job Role:** _____

Authoriser Signature: _____ **Date:** _____

Appendix E

St Thomas More High School

School Gateway Usage Policy

Introduction

This Policy applies wherever access to the St Thomas More High School, School Gateway is provided. This policy applies whenever information is accessed through the School Gateway, whether the computer equipment used is owned by St Thomas More High School or not. The policy applies to all those who make use of the School Gateway.

1. **Security**
   This policy is intended to minimise security risks. These risks might affect the integrity of St Thomas More High School's data, the authorised School Gateway user, and the individuals to which the School Gateway data pertains. In particular, these risks arise from:

   - The intentional or unintentional disclosure of login credentials to the School Gateway by authorised users.
   - The wrongful disclosure of private, sensitive, and confidential information.
   - Exposure of St Thomas More High School to vicarious liability for information wrongfully disclosed by authorised users.

2. **Data Access**
   This policy aims to ensure all relevant aspects of the General Data Protection Regulation and Privacy Notice are adhered to.

   This Policy aims to promote best use of the School Gateway to further the communication and freedom of information between St Thomas More High School staff, pupils, parents, and guardians.

3. **Authorised users**
   St Thomas More High Schools School Gateway is provided for use only by staff employed by the school, persons who are legally responsible for pupil(s) currently attending the school and those pupils. Access is granted only on condition that the individual formally agrees to the terms of this policy. The authorising member of school staff must confirm that there is a legitimate entitlement to access information.

4. **Personal use**
   Information made available through the School Gateway is confidential and protected by law under the General Data Protection Regulation. To that aim:

   - Users must not distribute or disclose any information obtained from the School Gateway to any person(s) with the exception of the pupil to which the information relates or to other adults with parental responsibility or authorised staff employed by the school.
   - Users should not attempt to access the School Gateway in any environment where the security of the information contained in the School Gateway may be placed at risk e.g. Internet Café.

5. Personal Identification Numbers (PIN)

You must assume personal responsibility for your School Gateway login credentials. Never use anyone else's account credentials.

You must always keep your individual PIN confidential. This PIN should ***never*** be disclosed to anyone. Account login credentials should never be shared.

The account requirements for the School Gateway are as follows:

- The email address used to register an account must be the same as that associated with your details held on the school's information management system.
- The mobile telephone number used to register an account must be the same as that associated with your details held on the school's information management system.

Only if the prerequisites above are met will it be possible to obtain a PIN number to log into the School Gateway.

Personal Identification Numbers (PIN) will not be disclosed via telephone conversation or email.

6. Questions, Complaints and Appeals

Users should address any complaints or enquiries about the School Gateway in writing or by email to St Thomas More High School at the following address: office@st-thomasmore.southend.sch.uk

St Thomas More High School reserves the right to revoke or deny access to the School Gateway of any individual under the following circumstances:

- The validity of parental responsibility is questioned.
- Court ruling preventing access to child or family members is issued.
- Users found to be in breach of this usage policy.

If any child protection concerns are raised or disputes occur, the school will revoke access for all parties concerned pending investigation.

Please note: Where School Gateway access is not available; St Thomas More High School will still make information available according to General Data Protection Regulation (GDPR) law.

7. Revision History

Version 1.0	20th March 2015	Initial Version
Version 1.1	13th March 2016	Policy Review
Version 1.2	22nd May 2018	Policy Review Update to data access to reference GDPR (2). Update to personal use to reference GDPR (4). Update to questions, complaints and appeals to reference GDPR (6). Addition of revision history (7).
Version 1.3	23rd October 2019	Policy Review. No Changes.
Version 1.4	6th September 2021	Policy Review. No Changes.
Version 1.5	27th October 2022	Policy Review. No Changes.
Version 1.6	8th September 2023	Policy Review. No Changes.
Version 1.7	24th September 2024	Policy Review. No Changes.

Appendix F

St Thomas More High School

CCTV Code of Practice and Usage Procedure

This CCTV Code of Practice and Usage Procedure for St Thomas More High School should be read and implemented in conjunction with the Assisi Catholic Trust CCTV Policy.

1. **Ownership and Operation**
   The CCTV systems, all recorded material and copyright is owned by St Thomas More High School. The system is operated by the Site, IT Technical and Pupil Support Departments whose personnel are employed directly by St Thomas More High School. The IT Manager is the officer of the School designated as having responsibility for the CCTV system and its operation.

   1.1 Operators
   Operators are members of staff that are authorised to review recorded images. These include:

   - Headteacher and his/her deputy
   - Director of Finance and Operations and his/her deputy
   - Assistant Headteacher - Attendance and Safeguarding
   - Pupil Support Mentors
   - Pupil Support Assistants
   - IT Manager and his/her deputy

   1.2 Monitors
   Monitors are members of staff that are authorised to view live video footage at designated monitoring stations. These include:

   - Site Team Staff

2. **Maintenance**
   Maintenance of the CCTV system will be carried out annually to ensure that it is operating in accordance with its purpose. A maintenance contract is held with 'School Watch'.

3. **Control Rooms**
   CCTV images will be captured in the Data Centre. CCTV images will be monitored in the Pupil Support Offices, the Site Team Workshop, Headteachers office and IT Support Team area. Access to the monitoring and recording facilities will be prohibited except for lawful, proper, and sufficient reasons and only by staff outlined in this Code of Practice and Usage Procedure or by law enforcement or inspection agencies and only then with the personal authority (verbal or written) of the Headteacher, his/her deputy or the Director of Finance and Operations. Any such visits will be conducted and recorded in accordance with School security procedures.

   Regardless of status, all persons visiting the Data Centre with the purpose of viewing recorded data will be required to sign the logbook and a declaration of confidentiality. Any other personnel admitted must be authorised by the Headteacher, his/her deputy or Director of Finance and Operations, or IT Manager (verbally or written).

4. Monitoring and Review

This CCTV Code of Practice and Usage Procedure will be kept under continuous review. Any questions about its interpretation or operation should be referred to the Headteacher.

5. Revision History

Version 1.0	6th March 2012	Draft
Version 1.1	22nd March 2012	Draft
Version 1.2	20th September 2012	Draft
Version 1.3	26th September 2012	Draft
Version 1.4	29th January 2013	Initial Version
Version 1.5	18th March 2016	Maintenance contract company change (10).
Version 1.6	31st March 2017	Policy review Revision of operators to include ICT Technical Manager Deputy (3.1). Removal of obsolete Reception Monitors references (3.2). Removal of obsolete Control Room references (16).
Version 1.7	22nd May 2018	Policy Review Revision of Data Protection Guidance in line with new legislation (1). Update to staff designated as having responsibility for CCTV (3). Update to period in which maintenance of CCTV system occurs (10). Update to processing data to reference GDPR (11). Update to period of time data will be held (12.1). Update to staff designated as contact for disclosure of data (13). Removal of 21-day notice period for subject access requests (14). Update to third party requests to reference GDPR (15). Removal of CCTV Code of Practise date reference (20).
Version 1.8	23rd October 2019	Policy Review Minor spelling and grammatical changes throughout.
Version 1.9	6th September 2021	Policy Review. No Changes.
Version 1.10	10th October 2021	Policy renamed to CCTV Code of Practice & Usage Procedure. Updated to co-exist with the Assisi Catholic Trust CCTV Policy. Section 1, 2, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 17, 18 and 20 removed.
Version 1.11	27th October 2022	Policy Review. No Changes.
Version 1.12	8th September 2023	Policy Review. Updated section 1.1 Operators to include Pupil Support Assistants and remove reference to Site Manager. Updated section 3 Control Rooms to remove reference to Site Manager, add Pupil Support Offices as a location where CCTV footage is viewed and remove reference to keys to the 'Control Room'.
Version 1.13	24th September 2024	Policy Review. Updated section 1.1 Operators to include Assistant Headteacher - Attendance and Safeguarding. Updated section 3 Control Rooms to include 'IT Support Team Area'.

Appendix G

Safe Use of Images Guidance Policy

Generally, photographs and videos for school and family use should be a source of innocent pleasure and pride, which can enhance self-esteem for children and young people and their families. Regrettably, there are occasions when this is not the case and technology such as digital and mobile phone cameras have made the potential for misuse of images easier. The following guidance is intended to apply to all forms of images, whether in print, on film or video, in digital form such as DVD, on websites and in the professional media.

1. Introduction

1.1 Photographs and videos can be effective ways to show parents and the local community the activities and learning that take place at our school.

1.2 Using new technologies such as digital cameras and websites makes it easier to take images and show them to the world, but we have a responsibility to make sure that individual and parental rights are respected, and that vulnerable individuals are protected from risk.

1.3 Issues of child protection, data protection and parental consent need careful thought. Images can be used by those who intend harm to children, for example as a preliminary to "grooming" or by displaying them inappropriately on the internet. The risk for an individual child is slight. However, for children that are abused in this way the consequences can be profound.

1.4 It is important to make a balanced judgement on the use of images. Schools are as likely to be criticised for over-reacting as they are for having failed to exercise caution.

2. Getting consent for the use of images of children and young people

2.1 The taking of photographs and videos of children purely for personal use such as by parents at Sports Day or by grandparent's videoing a play is not a breach of the General Data Protection Regulation and is not forbidden by the school.

2.2 Photographs taken for official use may be subject to the provisions of the General Data Protection Regulation. Permission from the person with parental responsibility for a child will therefore be sought before we take their photograph for a publication, website or display in a public place. A public place includes areas where visitors to our school have access.

2.3 The school will get consent to last for the whole period that the child is at school and the year after they have left, to enable us to publicise activities undertaken by final year students. (This is not intended to refer to photographs/videos around the school for the interest of the students. Many of these will show the 'history' of the school, e.g., school plays, sporting achievements etc.).

2.4 The school will send a consent form with the school's registration pack. Yearly reminders will be sent to all parents that they should let us know if there are changed circumstances, or if they want to withdraw permission for their child to be photographed. This reminder will be an annual standing item in a newsletter, e.g., 'Contact'. Parents retain the right to withdraw consent at any time. The school is obliged to comply with the parents and carers wishes.

2.5 If the two parents/carers disagree over consent for their child to appear in photographs or videos, we shall treat it as if consent has not been given.

2.6 Where children are in Public Care (Looked After) the school will gain consent on the corporate parent's behalf via the child/young person's social worker.

3. Getting Consent for adults

3.1 The school will seek written permissions from teachers, support staff, helpers, and volunteers to use their photographs.

4. Planning the use of images

4.1 The school will make sure that people are aware if the school intends to use their photograph in a potentially sensitive publication.

4.2 The school will take care to ensure that only images of students in suitable dress are taken, to reduce the risk of images being used inappropriately. The school will screen all images for acceptability, and if there is any possibility that a photograph could be used inappropriately then it will be destroyed. Particular care will be taken with photographs taken during PE and swimming lessons to maintain modesty.

4.3 No images should be taken of children/young people which capture them in what are commonly understood as non-public activities such as changing clothes or toileting, or which show body parts not usually visible in public settings.

4.4 The school will make sure that photograph shoots are inclusive, showing children/young people from a range of diverse backgrounds and abilities.

4.5 There may be occasions when a child/young person or his/her parent's security is a known risk (i.e., some adoption placements or child resettled after domestic abuse). In such circumstances, a child/young person will not appear in any photograph or image.

5. School plays and other events

5.1 Generally speaking, photograph/video recording will be permitted at school events. The one clear exception to this general rule will be for the congregation at Mass. There may be occasions when the school does not allow photography/video recording. This may be for a variety of reasons, for example:

- Disturbance to other members of the audience
- Distraction to the children taking part in a performance, especially where flash is used.
- Parental objection
- Child protection concerns

5.2 Parents, carers and their families can use photographs and videos taken at a school event for their own personal use. Such photographs and videos cannot be sold and must not be uploaded to the Internet, as that would contravene data protection legislation.

5.3 The school will make all parents/carers aware in advance of the event that other parents may want to video or photograph performances as a record of their child's work or performance.

5.4 The school will include a line in a letter home or include the "Use your camera courteously" code to make people aware that other parents may be recording the event.

5.5 If an objection is raised, the school shall need to consider ways to overcome this.

6. School fetes and open evenings

6.1 If the school is going to take general shots, at these events, of students and visitors for publicity purposes, the school should warn people in the invitations we send out that this will take place, so that general consent is implied by attendance.

7. Outside Events

7.1 Students may take part in public performances outside the school. In these cases, the event organiser should seek the permission of parents and carers for photographs to be taken and used in publicity.

8. Press Photography and Media Filming

8.1 The media operate under their own Code of Practice.

8.2 Students should not be approached or photographed at school without the permission of the school's authorities, however, we may want to invite the media into school to publicise an event or we may be approached by the media regarding a news story.

8.3 Newspapers will often want to name children in photographs – their first name and surname, and often their age as well. For this reason, it is important that the school makes parents/carers aware of this and give them an opportunity to object to their child being in media photographs.

8.4 If we invite the media into the school for publicity purposes, it is important that we inform parents/carers whose children may feature in photographs or filming.

8.5 If we know there are children who should not be identified as going to the school even if they are in a big group-shoot and are not named, we will need to keep them away from the cameras.

Any school suspecting a person of taking unauthorised photographs, or undertaking unauthorised filming of children, should immediately contact Essex Police.

9. Video Conferencing

9.1 The school will need to explain to parents how this is used and why, and that it means sending images over the internet that might be stored for educational use in schools. If parents/carers have not given permission for internet publication of their child's photograph, the school will need to angle the webcam to avoid these children.

10. Mobile Phones

10.1 Virtually all mobile phones now contain a facility to take photographs and videos and to transmit images taken, including uploading them onto the internet.

10.2 The same rules would apply as for photographs: users need to recognise that any pictures taken are for personal use only. (See guidelines for appropriate use of mobile phones).

11. CCTV

11.8 The school has installed closed circuit television (CCTV) as a security measure the school must operate this in accordance with the principles of data protection. Guidance on use can be found in our CCTV Code of Practice and usage policy.

12. Storage of Images

12.1 All photographs/video recording will be stored in a secure place and is only accessed by people who are authorised to do so. Digital images such as those used for student passes should also be stored securely, including any images stored on CD or other disks and on the school's computer network. Electronic images should be stored on media that is encrypted. The school will take care to ensure that it will not re-use photographs for more than a year after the student leaves the school.

12.2 When the school destroys photographs, it is important to destroy the negatives as well, and in the case of CDs and other media that cannot be erased electronically; the school should render the disk unusable.

13. Risk Assessment for PE and Other School Changing Rooms

13.1 A school risk assessment has been written and put in place to ensure student changing in the PE and other changing areas cannot be filmed or pictures taken.

13.2 PE and other relevant staff have read and signed off that they understand the policy.

14. Revision History

Version 1.0	23rd October 2019	Original policy document
Version 1.1	23rd October 2019	Policy Review Addition of version number and header. Addition of revision history (14).
Version 1.2	6th September 2021	Policy Review. No Changes.
Version 1.3	27th October 2022	Policy Review. No Changes.
Version 1.4	8th September 2023	Policy Review. No Changes.
Version 1.5	24th September 2024	Policy Review. Section 12.1 updated from 'Password Protected' to 'Encrypted'. Appendix 2 updated to reference 'Headteacher'.

Appendix 1

A checklist for schools when planning events at which photography and video could be used.

- Decide if you will permit photography and videoing at the event, however, remember that the taking of photographs and videos of children by their family purely for personal use should be allowed.
- When informing parents of the event, also inform parents/carers of your decision on photography and videoing.
- Including written guidance for parents/carers to the effect that any images must be taken for personal use only and specify that the images must not be put on the Internet otherwise data protection legislation will be contravened.
- Send a copy to all parents/carers of the 'Use your camera courteously' code.
- Most parents would expect to be asked to turn off their mobile phones during a performance for audio reasons, so remind them of the need to turn off for visual reasons also.
- Remind parents/carers with a verbal announcement at the start of the event that any images must be taken for personal use only and remind them that such images must not be put on the Internet otherwise data protection legislation will be contravened.
- Plan and think ahead as to where and when in the performance or event photographs and videos may be taken and give parents/carers attending the event appropriate guidance regarding where and when photographs may be taken. This will help to avoid disruption or distraction to the children, other parents, or staff.

- Be sure that parents and carers helping with children dressing or changing do not take photographs or videos whilst assisting with this.
- Be sure that people with no connection with your school do not have any opportunity to film covertly – remember to ask your staff to quiz anyone they do not recognise who is using a camera and/or video recorder at events and productions.
- If a video is produced by the school of a production, which includes a cast list in the credits, remember to revisit the parents of the cast to seek consent for names to appear, as this will enable children to be identified and could breach your policy.
- Members of staff should not store student photos on their personal computers at home or their school computers (unless acting purely as a parent). These should be stored centrally on the school system managed by the named person in the main office.

Appendix 2

The following is to be offered to parents as part of the letter/newsletter promoting the event:

Use your camera courteously.

Generally, photographs and videos for school and family use are a source of innocent pleasure and pride, which can enhance self-esteem for children and young people and their families. By following some simple guidelines, we can use such materials safely and with regard to the law.

- Remember that parents and carers attend school events at the invitation of the Headteacher and governors.
- The Headteacher and governors have the responsibility to decide if photography and videoing of school performances is permitted.
- The Headteacher and governors have the responsibility to decide the conditions that apply in order that children are kept safe, and that the performance is not disrupted, and children and staff not distracted.
- Parents, carers, and their families can use photographs and videos taken at the school event for their own personal use only. Such photographs and videos cannot be sold and must not be put on the Internet as that would contravene data protection legislation.
- Recording and/or photographing other than for private use would require the consent of all the other parents whose children may be included in the images.
- Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity. Restrictions on photography also apply to video and camera phones.
- We ask you to turn off mobile and camera phones during the performance to prevent disrupting it.
- Parents and carers must not photograph or video children changing for performances or events or in areas not designated by the schools as being acceptable.
- If you are accompanied by people that staff do not recognise, they may need to check who they are if they are using a camera or video recorder.

Appendix H

Use of Mobile Phones and Social Media Guidance Policy

The use of mobile phones in the school setting and the procedures for use in place are included within the schools E-Safety Policy.

1. Staff use of their own personal mobile phone within the school

1.1 Staff, both teaching and support staff are permitted to bring their own mobile phone onto the school premises or on a school related activity out of school.

1.2 Staff are however advised they should not use mobile phones for personal use near students, namely in teaching classrooms, school corridors, or whilst on a formal duty.

1.3 Considerate use of mobile phones is permitted for personal use in the staff room, private offices, out of school hours and when not with students.

1.4 Any school data stored on personal technology should be encrypted. Please refer to 'The ICT Usage and Code of Practice for Staff'.

1.5 Any inappropriate use may lead to disciplinary action.

1.6 Staff bring mobile phones into school at their own risk and should be prudent where they store them when not in use. Storage in teachers' desks in classrooms is not advised.

1.7 In the event that a member of staff is expecting an emergency call, staff should attempt to arrange the call to come through reception and normal channels or to receive the call in private without compromising the duty of care for their students under their supervision at that time.

2. Staff use of work issued mobile phones

2.1 A school mobile may be supplied to group leaders on school trips or outside activities for use in the smooth running of the trip or in the event of an emergency.

2.2 The mobile will, at all times, be kept secure by the group leader or a reliable nominated adult.

2.3 Students should not use a school phone unless supervised for a specific task.

2.4 The emergency school phone number can be given to students and parents for emergency contact purposes.

2.5 If staff elect to store contact numbers for their trip on the school mobile for emergency purposes, the member of staff should delete those numbers once the trip has been completed.

2.6 Confidentiality of the information stored on the mobile phone is secured by the group leader keeping the mobile safe and not accessible to unauthorised users.

2.7 School mobile phones provided to staff for any other purpose should adhere to this guidance.

3. Student use of mobile phones

3.1 Mobile phones should not be brought into school. The decision to provide your child with a mobile phone to give parents/carers reassurance that they can contact their child whilst travelling alone on public transport or journeys to and from school, is made on the understanding that the phone should be switched off completely whilst at school, not merely silenced or on divert or vibrate.

3.2 In order to reduce the risk of theft or loss during the school day, students who carry mobile phones must keep them concealed, not advertise that they have them, and mark them clearly with their name.

3.3 During examinations, we will continue to follow JCQ guidance (as found on the school website).

3.4 St Thomas More, the Governing Committee and school staff accept no responsibility for replacing mobile phones that are lost, stolen or damaged whilst on or travelling to the school premises, or on school sponsored functions.

3.5 If a student is seen with, or seen using a mobile phone on school premises, the phone will be confiscated to a secure place in school and returned at the end of the school day and a letter will be sent home on a first offence. If a student breaks this rule again, the phone will be confiscated to a secure place in school, parents/carers will be informed who then may collect the phone during office hours. Repeated infringements would be seen as a breach of the Student Behaviour Policy and sanctions may follow.

3.6 It should be noted that it is a criminal offence to use a mobile phone to menace, harass, or offend another person. The school will involve the police if such an event occurs.

4. Parental use of mobile phones in the school

4.1 Parents should not use mobiles whilst in the school setting with the exception of the school reception, sporting events or out of school hours.

4.2 Any concerns related to parental use of mobiles such as volume or content may be raised by members of school staff.

4.3 The use of mobiles to take pictures or video activities is covered under the schools 'Safe use of Images Guidance Policy'.

5. Safer use of images guidance

5.1 The school has a 'Safe Use of Images Guidance Policy', which is reviewed and adopted by Governors annually.

5.2 The policy covers who can take photographs with reference to staff, parents, and outside agencies.

5.3 The policy refers to which images cannot be taken.

5.4 A consent form is signed by all parents of students in school who give permission to have their son or daughter photographed. This consent outlines how photographs may be used in the school setting.

5.5 All school photographs are confidentially stored.

5.6 Parental permission for photographs to be taken are logged under student details on SIMS and highlighted in a separate column on the student trip list for each new trip that runs.

5.7 It is expected that the group leader is aware of which students in the group do not have permission for photographs to be taken.

5.8 No student is allowed on a school trip or activity unless the generic consent form has been returned.

6. Use of Social Media networking sites

6.1 The use of school equipment to access social networking sites for personal use is prohibited.

6.2 Only staff with school authorisation to access specific networking areas, such as Twitter, may do so.

6.3 Staff accessing social networking sites without authorisation on school equipment may face disciplinary action.

6.4 Staff should not use their personal equipment to access social networking sites in the school setting whilst near students, this includes whilst in the classroom, corridors, computer rooms or other public areas of the school and whilst on duty.

6.5 Appropriate use of electronic technology, using personal equipment may be undertaken in private areas of the school away from the vicinity of the students such as the staff room and offices.

6.6 Inappropriate use of social networking sites either within the school setting or within private time that brings the schools catholic ethos and good name into disrepute could lead to disciplinary action.

6.7 It is prohibited to 'friend' present students at the school on a social networking site such as Facebook unless it has been authorised by the school.

6.8 Staff should refer to the Safeguarding and Child Protection, and Safer Use of Images policies and refer to their terms and conditions of employment to ensure their actions do not bring the schools good name into disrepute.

6.9 Use of electronic technology whether within the school setting or out, should not compromise a member of staffs professional integrity.

7. Revision History

Version 1.0	23rd October 2019	Original policy document
Version 1.1	23rd October 2019	Policy Review Addition of revision history (7). Addition of version number and header. Formatted for easier reference. Headings updated with new terminology.
Version 1.2	6th September 2021	Policy Review. No Changes.
Version 1.3	27th October 2022	Policy Review. No Changes.
Version 1.4	8th September 2023	Policy Review. No Changes.
Version 1.5	24th September 2024	Policy Review Removal of section 2.7 as no longer relevant. Updated section 2.8 to section 2.7 to reference 'all staff'. Updated section 6.8 to reference correct policy names.

Appendix I

Filtering and Monitoring Policy

Filtering and monitoring systems are used to keep pupils safe when using the school's IT system.

- Filtering systems: block access to harmful sites and content.
- Monitoring systems: identify when a user accesses or searches for certain types of harmful content on school devices (it doesn't stop someone accessing it). The school is then alerted to any concerning content to intervene and respond.

No filtering and monitoring system is 100% effective, so will be used alongside existing safeguarding systems and procedures.

1. Roles and Responsibilities

1.1 All staff should be clear on:

- The expectations, applicable roles, and responsibilities, in relation to filtering and monitoring as part of their safeguarding training. For example, part of their role may be to monitor what's on pupils' screens.
- How to report safeguarding and technical concerns, such as if:
  - They witness or suspect unsuitable material has been accessed.
  - They are able to access unsuitable material.
  - They are teaching topics that could create unusual activity on the filtering logs.
  - There is failure in the software or abuse of the system.
  - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
  - They notice abbreviations or misspellings that allow access to restricted material.

1.2 Senior leaders and all relevant staff need to be aware of and understand:

- What provisions the school has in place and how to manage these provisions effectively.
- How to escalate concerns when they identify them.

1.3 Senior leaders are also responsible for:

- Buying-in the filtering and monitoring system the school uses.
- Documenting what is blocked or allowed, and why.
- Reviewing the effectiveness of the provision, making sure that incidents are urgently picked up, acted on and outcomes are recorded.
- Overseeing reports.
- Making sure staff are trained appropriately and understand their role.

1.4 The DSL should take lead responsibility for online safety, including understanding the filtering and monitoring systems and processes in place, this is part of their role in taking the lead responsibility for safeguarding. This includes overseeing and acting on:

- Filtering and monitoring reports.
- Safeguarding concerns.
- Checks to filtering and monitoring systems.

2. Filtering and Monitoring

2.1 The school will identify and assign roles and responsibilities to manage filtering and monitoring systems.

2.2 Review filtering and monitoring provision at least annually.

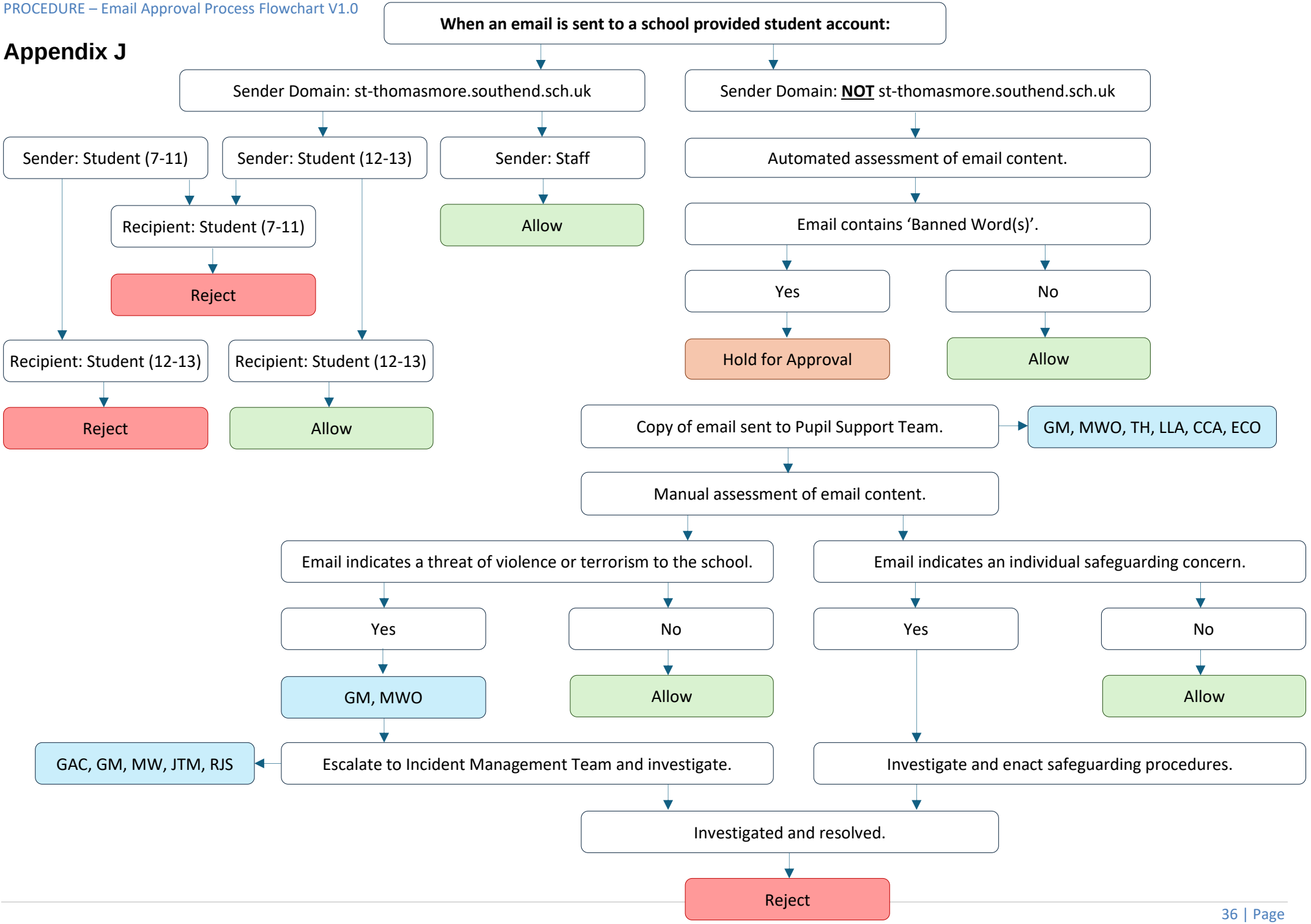
2.3 Block harmful and inappropriate content without unreasonably impacting teaching and learning.

2.4 Have effective monitoring strategies in place that meet safeguarding requirements.

3. Revision History

Version 1.0	8th September 2023	Initial version
Version 1.1	24th September 2024	Policy Review. No Changes.

Appendix J


When an email is sent to a school provided student account:
Sender Domain: st-thomasmore.southend.sch.uk
Sender Domain: NOT st-thomasmore.southend.sch.uk
Sender: Student (7-11)
Sender: Student (12-13)
Sender: Staff
Automated assessment of email content.
Recipient: Student (7-11)
Allow
Email contains 'Banned Word(s)'.
Reject
Yes
No
Recipient: Student (12-13)
Recipient: Student (12-13)
Hold for Approval
Allow
Reject
Allow
Copy of email sent to Pupil Support Team.
GM, MWO, TH, LLA, CCA, ECO
Manual assessment of email content.
Email indicates a threat of violence or terrorism to the school.
Email indicates an individual safeguarding concern.
Yes
No
Yes
No
GM, MWO
Allow
Allow
GAC, GM, MW, JTM, RJS
Escalate to Incident Management Team and investigate.
Investigate and enact safeguarding procedures.
Investigated and resolved.
Reject