St Thomas More RC College

Policy:

E-Safety Policy / Acceptable Use Policy (AUP)

This policy will be reviewed every 12 months

Author	J Kirk

	Signature of member of Governing body	Date
Policy approved/ reviewed (delete as appropriate)		21 February 2024

Rationale
Technology has become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. However, the use of these technologies can put young people at risk. They should have an entitlement to safe internet access at all times. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content.
• Unauthorised access to/loss of/sharing of personal information.
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing/distribution of personal images/videos without an individual's consent or knowledge.
• Inappropriate communication/contact with others, including strangers.
• Cyber-bullying.
• Access to unsuitable websites, videos & internet games.
• An inability to evaluate the quality, accuracy and relevance of information on the internet.
• Plagiarism and copyright infringement.
• Illegal downloading of music or inappropriate video files.
• Excessive use of screentime and online access which may impact on the social and emotional development and learning of the young person.
• Youth produced imagery.
• Upskirting.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

This Policy should help to ensure safe and appropriate use and to encourage pupils to grow into discerning and responsible users and should be read in conjunction with the Child Protection Policy, the Anti-Bullying Policy and the Behaviour Policy.

This e-safety policy has been developed by the E-safety Team made up of:

Position	Name(s)
Head of Learning Support	Joanne Kirk Child Protection Teacher
Curriculum Leader – Computer Science	Adam Jennings
Curriculum Leader – CPSHE	Liam Wright
HLTA Inclusion	Vacancy
HLTA Inclusion	Kiayah Nolan
IT Manager	Dataspire

Consultation with the whole college community has taken place through the following:

Staff meetings
INSET Day – Annual Staff Training – Staff sign Safeguarding Agreement

This policy applies to all members of the college community (including governors, staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the college ICT systems and mobile technologies, both in and out of college.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the college:

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Head Teacher and Senior Leaders:

- The Head Teacher/Deputy Head Teacher are responsible for ensuring the safety (including e-safety) of members of the college community.
- The Head Teacher and the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Team:

- Members of the E-safety Team will assist the E-Safety Coordinator with the production, review and monitoring of the college e-safety policy on an annual basis.

(Child Protection Teacher) Joanne Kirk:

- leads the e-safety Team and college initiative on e-safety.
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the college e-safety policies.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- reports regularly to the Senior Leadership Team**.**

Joanne Kirk is trained in e-safety issues and is aware of the potential for serious Child Protection issues to arise from:

- sharing of personal data.
- access to illegal/inappropriate/ extremist materials.
- inappropriate on-line contact with adults/strangers.
- potential or actual incidents of grooming e.g. Child Sexual Exploitation, radicalisation.
- cyber-bullying.

Network Manager / Technical staff:

Dataspire is responsible for ensuring:

- that the college's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the college meets the e-safety technical requirements outlined in any relevant Government/DfE and Local Authority guidance.
- that users may only access the college's networks through a properly enforced password protection and AUP policy.
- that security, safeguarding and filtering systems are suitable and up to date.
- that the college cloud/ internet-based services are suitably secured
- that appropriate backup solutions are in place and regularly tested.
- ensuring the college complies with data protection and GDPR regulations.

Teaching and Support Staff:

are responsible for ensuring that:

- they have an up to date awareness of data protection and e-safety matters and of the current college e-safety policy and practices.
- they have read, understood and electronically signed the college Staff Acceptable Use Policy/Agreement (AUP), at the beginning of each half term.
- they report any suspected misuse or problem to the E-Safety Co-ordinator (J Kirk) for investigation/action/sanction.
- they have read all relevant safeguarding documents and signed to confirm this annually.

Pupils:

- are responsible for using the college ICT systems and mobile technologies in accordance with the Pupil Acceptable Use Policy, which they sign electronically when logging in to college systems.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so and who to report to.

Parents/Carers

The college will take every opportunity to help parents understand these issues through website information about national/local e-safety campaigns. Parents and carers will be responsible for:

- endorsing (by signature) the STM Student IT Services Agreement as part of the admission process.
- accessing the college ICT systems in accordance with the procedures set out within this policy.

Communication devices and methods

The following table shows the college's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				Pupils			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	☑	⚠	⚠	☒	☑	⚠	⚠	☒
Mobile phones may be brought to college	☑				☑			
Use of mobile phones in lessons		⚠						☒
Use of mobile phones in social time	☑							☒
Taking photos or videos on personal mobile phones or other camera devices				☒				☒
Interactive use of wearable electronic devices e.g. Smart watches	☑							☒
Use of tablet devices	☑						⚠	
Use of personal email addresses in college, or on college network		⚠						☒
Use of college email for personal emails				☒				☒
Use of online meetings (Teams, Zoom, Satchel One) chat rooms / messaging facilities for educational purposes	☑						⚠	
Use of social networking sites				☒				☒

Use of educational blogs/vblogs (YouTube etc)	☑							

 This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Pupils**
Mobile phones may be brought to college		To contact parents in an emergency with a member of staff present. Otherwise must be switched off at all times.
Use of mobile phones in social time	During breaks/lunch or after college	
Use of personal tablets and handheld devices	As a teaching resource	As a focused learning resource, monitored by teachers
Use of personal email addresses in college, or on college network	During breaks/lunch or after college	
Use of college email for personal emails	College emails are not to be used for personal business and communication.	As a learning resource to send work home and collaborate with other students
Use of online meetings (Teams, Zoom, Satchel One) chat rooms / messaging facilities for educational purposes	Contact staff within school, or to communicate with external agencies e.g. webinars (training)	As a learning resource in lessons
Use of educational blogs/vblogs (YouTube etc)	Access teaching resources	Use as a learning tool.

Unsuitable/inappropriate activities using college internet & devices

The college believes that the activities referred to in the following section would be inappropriate in a college context and that users, as defined below, should not engage in these activities in college or outside college when using college equipment or systems. Internet access on site is monitored and filtered, in order to restrict access to inappropriate material. The college policy restricts certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users (staff)	Unacceptable	Unacceptable and illegal
User Actions	☑			☒	☒
child sexual abuse images					☒
promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					☒
adult material that potentially breaches the Obscene Publications Act in the UK					☒
criminally racist material in UK					☒
Extremist materials					☒
Pornography					☒
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					☒
promotion of racial or religious hatred					☒
threatening behaviour, including promotion of physical violence or mental harm					☒
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute				☒	
Using college systems to run a private business				☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the college				☒	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☒	

Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					☒
Creating or propagating computer viruses or other harmful files					☒
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☒	
On-line gaming (educational)		⚠			
On-line gaming (non-educational)				☒	
On-line gambling				☒	
Accessing the internet for personal or social use (e.g. online shopping, banking etc.)			⚠		
File sharing e.g. music, films etc.				☒	
Use of social networking sites			⚠	☒	
Use of video broadcasting e.g. YouTube		⚠			
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)				☒	
The storage of sensitive/inappropriate documents/media files of any description on the college cloud-based storage solutions					☒

 This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
User Actions	**Staff & other adults**	**Students/Pupils**
On-line gaming (educational)		as a learning resource
Accessing the internet for personal or social use (e.g. online shopping, banking etc.)	during break/ lunch times and in personal time	
File sharing e.g. music, films etc.		only if copyright-free and being used as a learning resource
Use of video broadcasting e.g. YouTube	for showing educational videos	as a learning resource, to access tutorials
Using external data storage devices (e.g. USB/Cloud based storage) that have not been encrypted (password protected and checked for viruses)	used to save teaching and learning materials only for use at home	used to save work for home learning

Good practice guidelines

Email

Best practice

☑ DO

Staff and students/pupils should only use their college email account to communicate with each other

Safe practice

Check the college e-safety policy regarding use of your college email or the internet for personal use e.g. shopping

Poor practice

☒ DO NOT

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

Images, photos and videos (media files)

Best practice

☑ DO

Only use college equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Head Teacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the college network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Head Teacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Appropriate Internet Use

Best practice

☑ **DO**

Understand how to search safely online and how to report inappropriate content.

Safe practice

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. Any inappropriate usage will be recorded and appropriate sanctions put in place.

Poor practice

☒ **DO NOT**

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones

Best practice

☑ **DO**

Staff: *If you need to use a mobile phone while on college business (trips etc.), the college will should provide equipment for you.*

Make sure you are aware of app content and facilities.
Staff: *Good practice is to have phone on silent.*
Pupils: *Phones should be switched off at all times and kept securely in bags.*

Safe practice

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Disable caller-ID if using to phone to contact external agencies or parents/carers

Poor practice

☒ **DO NOT**

Staff: Don't use your own phone without the Head Teacher/SLT knowledge or permission.

Don't retain student/pupil/parental contact details for your personal use.

Social Media Sites (various)

Best practice

☑ DO

Check all settings and make sure your privacy settings are set to 'Private'.

Ask family and friends to not post tagged images of you on 'Public' profiles.

Safe practice

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

☒ DO NOT

Don't have an 'Public' profile that includes inappropriate personal information and images, photos or videos.
Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.

Staff:
Don't accept ex-students/ pupils/ parents as friends.

Don't write inappropriate or indiscrete posts about the college, colleagues, students/pupils or their parents.

Webcams/Smartphone Cameras

Best practice

☑ DO

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Head teacher/SLT knowledge or permission

Plan for pictures saved to be downloaded to the college network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Head Teacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Incident Management

Incidents (PUPILS):	Refer to e-safety Team	Refer to class teacher	Refer to Head of Department / PAL	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unauthorised use of non-educational sites during lessons		☑							☑	☑
Unauthorised use of mobile phone/digital camera / other handheld device		☑					☑			☑
Unauthorised use of social media/ instant messaging/personal email		☑	☑							☑
Unauthorised downloading or uploading of files		☑				☑		☑		☑
Allowing others to access college network by sharing username and passwords			☑				☑	☑		☑
Attempting to access or accessing the college network, using another student's/pupil's account	☑					☑	☑	☑		☑
Attempting to access or accessing the college network, using the someone else's account other than your own.	☑		☑			☑	☑	☑		☑
Corrupting or destroying the data of other users						☑				☑
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑		☑				☑			☑
Continued infringements of the above, following previous warnings or sanctions	☑			☑						
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college				☑			☑			
Using proxy sites/VPNs or other means to subvert the college's filtering system	☑			☑		☑	☑			☑
Accidentally accessing offensive/ extremist or pornographic material and failing to report the incident	☑		☑			☑	☑			

Deliberately accessing or trying to access offensive/ extremist or pornographic material	☑		☑	☑		☑	☑	☑		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		☑								

Incidents (STAFF):	Refer to e-safety Team	Refer to Head of Department / Head of Year / other	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Warning	Further sanction *(AT HeadTeachers discretion)*
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	☑	☑	☑		☑		
Excessive or inappropriate personal use of the internet / social media sites / messaging / personal email accounts		☑	☑				
Unauthorised downloading or uploading of files	☑		☑		☑		
Allowing others to access college network by sharing username and passwords or attempting to access or accessing the college network, using another person's account	☑	☑	☑		☑		
Careless use of personal data eg holding or transferring data in an insecure manner					☑		
Deliberate actions to breach data protection or network security rules		☑	☑		☑		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		☑	☑		☑		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑	☑	☑		☑		
Making offensive or defamatory comments through social media or digital communications.			☑				
Using **personal** email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	☑	☑	☑		☑		
Actions which could compromise the staff member's professional standing			☑				

Actions which could bring the college into disrepute or breach the integrity of the ethos of the college			☑				
Using proxy/VPN sites or other means to subvert the college's filtering system		☑	☑		☑		
Accidentally accessing offensive or pornographic material and failing to report the incident							
Deliberately accessing or trying to access offensive or pornographic material	☑		☑	☑			
Breaching copyright or licensing regulations		☑					
Using college systems to run a private business			☑		☑		
Continued infringements of the above, following previous warnings or sanctions			☑				

Further Information

Staff - Using Social Media Responsibly

Your personal activities must not undermine the college's reputation, your professional reputation, or create perceptions of impropriety in the college, or bring the college in to disrepute.

TOP TIPS TO KEEP YOU SAFE (PLEASE READ CAREFULLY)

1) Do not "speak" for the college unless you have express permission…

- You should not "speak" for the college (disclose information, publish information, make commitments/comments or engage in activities on behalf of the college) unless you are specifically authorised to do so by the SLT.

- Any online activities associated with work for the college should be discussed and approved in advance by the SLT.

2) Keep confidential…

- Avoid sharing any confidential information about or dealings with the college, Governors, other employees, and/or members of the public unless you have express written permission from the SLT.

3) If you can be linked to the college act appropriately...

- Where you are clearly identifiable as being an employee of the college and/or discuss your work or college business using social media, you must behave appropriately and in ways that are consistent with the colleges values and policies, avoiding any activities which might bring the college into disrepute.

- Never make offensive or defamatory comments about any parents, children, members of staff or governors. Don't use ethnic slurs, personal insults, obscenity or behave in ways that would not be acceptable in the workplace which could bring the college into disrepute, break the law and leave you open to prosecution and/or disciplinary action.

4) Consider contact with pupils and parents carefully

- Ensure than any contact with pupils (current or former) is strictly within an educational context, if necessary at all.

- **You are strongly advised not to accept pupils as "friends" on social media sites** for your own protection, if you do liaise with pupils electronically, you are advised to do so using official college email accounts, or managed learning platforms, so that any communication is logged and can be monitored, and remains within the acceptable boundaries of that professional relationship.

- If you receive contact from a pupil (current or former), you are advised to inform your head teacher who will decide about informing their parent(s)/ carer(s), as there are specific rules which apply to use and misuse of social media sites for young people.

- If, despite your best efforts, your personal details fall into the wrong hands and a pupil (current or former) makes contact with you, you should let the SLT know and do not reciprocate this communication.

- Remember the boundaries of your professional relationship with pupils and ensure that your behaviour does not blur these boundaries.

5) Remember that colleagues, prospective employers, parents and children may see your online information…

- Whether you identify yourself as an employee of the college or not, think carefully about how much personal information you want to make public and make sure your profile and the information you post reflects how you want them to see you both personally and professionally.

- It is recommended that you apply the highest privacy settings and regularly review them, as the website may alter the setting without your knowledge.

- Ensure that anything you post is in accordance with the college's E-Safety Policy / Acceptable Use Policy (AUP) and your code of conduct.

- Be aware that inappropriate or derogatory comments about colleagues, Governors, parents or children could potentially lead to gross misconduct, which could ultimately result in dismissal.

6) Choose your "friends" carefully

- You may appear in photographs published by other people, and you may be identified without consent, for example by 'tagging' on Facebook, so you are advised to be mindful of what photographs you appear in.

- You can remove your identification from such photographs but not the photograph itself. Your 'friend' may not have as rigorous security settings as you might choose for yourself.

- If you find out that through no fault of your own, you have been identified in a way which might be in breach of these guidelines, you must take immediate steps to rectify the situation. For example, by contacting the person who published the information / image and asking them to remove it.

8) Stay legal

- Be aware that confidentiality, libel, defamation, copyright and data protection laws apply on-line just as in any other media.

- Remember you are personally liable for what you publish online.

3) Protect yourself from identity fraud...

- Restrict the amount of personal information that you give out.

<u>Attached Documents (to be used as needed)</u>

STM Student IT Services Agreement.docx