St. Thomas More Catholic Primary School

South Road, Saffron Walden, Essex. CB11 3DW
Email: admin@stmsw.co.uk
HEADTEACHER: Mrs. M.J. Hall M.Phil
Telephone: 01799 523248

St Thomas More Computing & Data Protection Policy

April 2023

St. Thomas More Catholic Primary School
South Road, Saffron Walden, Essex. CB11 3DW
Email: admin@stmsw.co.uk
HEADTEACHER: Mrs. M.J. Hall M.Phil
Telephone: 01799 523248

One of the most valuable facets of today's teaching is its inclusion of technology across the curriculum; both in lessons specifically focused on computing and as a resource in more traditional core subjects to further assist with learning and pupil development. As well as aiding in staff's best possible delivery of teaching. As a school, we will follow this policy in order to ensure that the computing facilities and resources on our site are used and maintained to provide the best possible level of support for all those involved. This policy will be adhered to by all employees of the school, all visitors, volunteers and any other user of computing related equipment or resources whilst on our school site.

All of St Thomas More's computing and technical equipment facilities and information resources remain the property of St Thomas More and not of particular teams, individuals or departments. By following this policy, we as a staff, ensure that the facilities are used:

- Legally
- Securely
- Without undermining the school or the wellbeing of its pupils
- Effectively
- In the spirit of co-operation, trust and consideration for others
- So that they remain available

1. Disciplinary Measures

1.1 Deliberate and serious breach of the policy statements in this section may lead to the school taking disciplinary measures in accordance with our Disciplinary Procedure Policy. The school accepts that computing – including access to the internet, Office 365 email system, Microsoft Teams and the Remote Desktop Server – are incredibly valuable assets and tools, but we also recognize that misuse of these facilitates can have a negative impact upon a user's productivity, and furthermore, the operation and/or reputation of the school.

1.2 In addition to the aforementioned statement, all of our school's phone, internet and email related services are provided for business and operating purposes. Therefore, as a school, we maintain the right to monitor the volume of internet and network traffic, alongside the email systems. The specific content of any of these communiques will not be directly monitored unless as a school, we believe the technology and/or resources are being misused.

2. Security

2.1 As a user of the physical equipment and digital resources provided by St Thomas More, you are solely responsible for your activity on our network.

2.2 Do not disclose personal system passwords or other security details to other employees, volunteers, external agents or pupils and do not use anyone else's log-in as this compromises the security of our network. If someone else learns of your password, ensure that you change it or request assistance in rectifying the situation from your Interm IT Consultant. Under no

circumstances are other users of the network, be they staff or students, allowed to use your K9 account for any purpose. All documentation requiring sharing should be kept in the shared spaces allocated on the school server.

2.3 Should you need to leave your computer unattended for any period of time, you **WILL** lock the screen to prevent unauthorized access to the network and the resources on that network. If you fail to do so, you will become responsible for any misuse of it while it is unattended. Be this the viewing or access of documentation, tools for learning or Office 365 services such as Outlook or Microsoft Teams.

2.4 To the best of your ability, external hard drives, USB drives ect should not be used. If these devices **MUST** be used (the use of the school RDS should deem these obsolete) they **MUST** be encrypted. It is solely your responsibility to ensure this.

2.5 Do not attempt to gain unauthorized access to information, resources or facilities on St Thomas More's School K9 network. The Computer Misuse Act 1990 makes it clear that it is a criminal offense to obtain unauthorized access to any computer (including workstations and laptops) or to modify their contents. If you do not have access to information or resources you feel you need to carry out the duty of your job role, contact your line manager who will inform your Interm IT consultant.

3. Use of Email

3.1. When to use email:

3.1.1. Use email in preference to paper to reach people quickly (therefore saving time on photocopying/distribution) and help contribute to the school's efforts to cut paper waste. Microsoft Teams can also be used for this purpose.

3.1.2. Use the phone for urgent messages (email is a good backup in some instances). Use of email by employees of the St Thomas More is permitted and encouraged where such use supports the goals and objectives of the school.

3.1.3 However, we do request that the use of email by employees and volunteers, complies with current legislation and guidance and the content/subject of emails do not create unnecessary business risk to the school, it's employees or pupils by misuse of this service.

3.2. Unacceptable behaviour:

3.2.1. Sending confidential information to external locations without the appropriate safeguards in place. See paragraph 5 of this document for more details.

3.2.2. Distributing, disseminating or storing images, text or other digital materials that might be considered indecent, pornographic, obscene or illegal.

3.2.3. Distributing, disseminating, or storing images, text or other digital materials that may in some way be considered discriminatory, offensive, abusive, sexist, racist or potentially considered harassment, bullying or defamation of character.

3.2.4. Using copyrighted information in such a way that the copyrights of those images or documents are violated.

3.2.5. Gaining unlawful access to St Thomas More or another organizations system or network or gaining unlawful accessinto a private mailbox or user area through the use of an obtained password or a screen that is left unsecured in the proper way.

3.2.6. Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

3.2.7. Transmitting or sharing unsolicited commercial or advertising related material.

3.2.8. Undertaking deliberate activities that waste another employee's time, effort or allocated network resources.

3.2.9. Deliberately or recklessly introducing any form of computer virus, malware or otherwise unvetted software onto the school's network.

3.3. Confidentiality

3.3.1 Always exercise caution when placing/committing/attaching confidential information to email or the internal network since through these systems, there is no guarantee that such materials will remain confidential. St Thomas More reserves the right to monitor **ALL** electronic communications in accordance with the relevant laws and policies. The right to monitor such communications includes messages sent or received by system users (employee'sand temporary staff such as cover or supply teachers) within and outside the system as well as messages that are deleted from the aforementioned systems. See paragraph 5 for more detail.

3.4. General points on Office 365 usage

3.4.1. When publishing or transmitting information externally please be aware that you are an acting representative of St Thomas More and this communique could be seen as speaking on behalf of the school. Make it clear when stated opinions are personal and if in doubt, contact your line manager.

3.4.2. To the best of your ability, check your emails and Microsoft Teams throughout your working day. Keep your inbox fairly empty so that it only contains items that require response or action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email to a specific folder or extract the information required and save it elsewhere.) This makes mailbox management quicker and easier on a daily basis.

3.4.3. Keep electronic files of electronic correspondence, only retaining what you actually need to. Do not print off emails and keep them in paper files unless completely necessary. This is a waste of resources and a potential risk to confidentiality.

3.4.4. Do not forward emails warning of viruses or malware (they are invariably hoaxes and your Interm IT Consultant will probably already be aware of genuine security or network concerns – if in doubt, contact them for advice)

3.4.5. Do not open an email unless you have a reasonable expectation of what it contains and do not download files unless they are from a trusted source. For example, open a report.doc from a colleague but don't download a similar file from an address you don't recognize from outside of your organization. It is your responsibility to act in order to mitigate risk to the network and it's security. If you receive any emails containing suspicious documentation or sent from addresses that concern you, alert your line manager and your Interm IT Consultant.

4. Use of the Internet

4.1. Use of the internet by employees and volunteers is permitted and encouraged where such use supports the learning of the pupils and the delivery of teaching within the school environment.

4.2. However, use of the internet is only permitted should employees ensure that they comply with the current legislation, use the internet in an acceptable way and do not create unnecessary risk to the school organization by any potential misuse of the internet.

4.3. Unacceptable Behavior

4.3.1. In particular, the following is deemed unacceptable use or behavior by employees and volunteers, this list includes but is not limited to;

4.3.1.1. Visiting internet sites which contain obscene, hateful, pornographic or other illegal material

4.3.1.2. Using the computer to perpetrate any form of fraud as well as software, film or music piracy.

4.3.1.3. Using the internet to send offensive or harassing material to other users.

4.3.1.4. Downloading commercial software or any copyrighted materials belonging to third parties: unless this download is covered or permitted under a commercial agreement or other such license held by the school.

4.3.1.5. Gaining access into unauthorized areas on the school network or any external network.

4.3.1.6. Creating or transmitting/sharing any form of defamatory material.

4.3.1.6. Undertaking deliberate activities that waste employees time, effort or networked resources.

4.3.1.7. Deliberating or recklessly introducing any form of computer virus and/or malware into the school's network.

4.4. Chat rooms / instant messaging (IM)

4.4.1. The use of chat rooms and instant messaging is strictly prohibited within working hours. This includes Facebook Messenger, Whatsapp's desktop clients and any form of messaging within Instagram and other similar social media sites.

St. Thomas More Catholic Primary School
South Road, Saffron Walden, Essex. CB11 3DW
Email: admin@stmsw.co.uk
HEADTEACHER: Mrs. M.J. Hall M.Phil
Telephone: 01799 523248

4.5. Obscenities

4.5.1. Do not write, publish, search for, look for, share, bookmark, access or download any materials that may in any way be regarded as obscene. Any use of obscenities is tracked and monitored via the schools Senso Safeguarding service, any breaches of this policy statement will be deferred to the Head Teacher and could potentially lead to disciplinary procedures.

4.6. Copyright

4.6.1. Take care to use software legally and in accordance with both the spirit and guidance of relevance licensing and copyright agreements. Copying software for use outside these agreements is strictly prohibited as it is illegal and may in incur criminal charges. This includes attempting to install any software requiring a license on the school network.

5. Confidentiality

5.1. If you are dealing with personal, sensitive and/or confidential information, then you must ensure that extra care is taken to protect the aforementioned information.

5.2. If sending personal, sensitive and/or confidential information via email, a number of protocols should be followed. If there is any doubt as to the information being sent or whether or not an appropriate level of protection has been applied, please check with the schools DPO (Data Protection Officer).

5.2.1. Personal, sensitive and / or confidential information should be contained within an attachment NOT within the main body of an email or the subject line of an email.

5.2.2. In appropriate cases, the attachment should be encrypted, and/or password protected, and any password or passkey must be sent separately to the appropriate party.

5.2.3. Before sending the email, verify the email address of the recipient and if you deem appropriate, telephone the recipient to check and inform them that the email will be sent.

5.2.4. Do not refer to the information contained in the secure attachment within the subject of the email.

6. St Thomas More's K9 Network

6.1. Keep master copies of any and all important data on the St Thomas More School's server (on the appropriate drive) and not solely on your desktop or laptop's local C: Drive or any other portable drive. Not storing data on the school's wider network means that it will not be backed up daily and therefore it is at risk of loss or potential corruption. Neither the school, nor it's support partners will be held liable for any documentation or data lost through improper network storage.

6.2. Ask for advice from your Interm IT Consultant should you need to store, transmit or handle large quantities of data, particularly images, audio or video. These large files take up disk space very quickly and add significant strain and stress to the network's daily operation. Therefore impacting it's use for students and staff.

6.3. Under no circumstances should you store any personal (Files/documentation not related to the school) files on the school's network, this is regardless of where this data will be stored.

Personal data is for personal devices.

6.4. Do not copy files that are accessible centrally into your personal directory or onto your personal drive, unless you have prior permission. (IE, if you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

7. Removable Media

7.1. If storing or transferring personal, sensitive, confidential or classified information using Removable Media you must contact the school's DPO or the Head Teacher for prior permission. Any use of removable media should be a last resort and anyone needing to access or use ANY internal documentation or systems at home, should use the schools Remote Desktop Server in order to do this.

7.1.1. Always consider that an alternative solution may already exist.

7.1.2. Only use recommended removable media.

7.1.3. Encrypt and password protect.

7.1.4. Store all removable media securely.

7.1.5. Removable media must be disposed of securely by the Network Manager or relevant technical team.

8. Personal use of ICT facilities

8.1. Social media: For the purposes of this policy, social websites are web-based and mobile technologies which will allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that due to the advances in technology this is a constantly changing area where sites regularly fall in and out of relevance and use.

8.1.1. **Use of Social Media at work**

8.1.1.1. Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from St Thomas More equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities. (I.E. Updating or managing your school's social media accounts from your workstation, at a school, these accounts are currently limited to Facebook and Twitter.)

8.1.1.2. Access to particular social media websites may be withdrawn in the case of misuse.

8.1.1.3. Inappropriate comments on social media websites can cause damage to the reputation of the organization if a person is recognized as being an employee or

volunteer. It is, therefore, imperative that you are respectful of the organization's service as whole including client's, colleagues and partners.

8.1.1.4. Employees and volunteers should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of St Thomas More unless appropriately authorized to do so. Personal opinions must be acknowledged as such and should not be represented in any way that might make them appear to be those of the organization. Where appropriate, an explicit disclaimer should be included for example 'These statements and opinions are my own and not those of the St Thomas More'.

8.1.1.5 At no point, in any public forum or on any social media should you 'tag' yourself as at the school, list yourself as being employed by the school or make comments that mention the school, it's staff, parents or pupils under any circumstances. This caveat applies to your own personal social media accounts and communique made in a personal capacity.

8.1.1.6. Any communications that employees or volunteers make in a personal capacity must not:

- Bring the St Thomas More into disrepute, for example by criticizing colleagues or partner organizations.
- Breaching the school's policy on confidentiality or any other relevant policy.
- Breach copyright, for example using someone else's images or written content without permission.
- Do anything which might be viewed as discriminatory against or harassment towards any individual, for example, by making offensive or derogatory comments relating to age, disability, gender reassignment, race, religion or belief, sex or sexual orientation.
- Use social media to bully, abuse, defame or harass another individual.
- Post images that are discriminatory or offensive or post links to such content.

8.1.2. St Thomas More maintains the right to monitor usage where there is suspicion of improper use.

8.2. Other personal use

8.2.1. Use of facilities on site for 'leisure' or personal purposes (e.g. sending and receiving personal email, making personal phone calls, browsing the internet and streaming media) is permitted as long as such use does not;

8.2.1.1. Incur specific financial expenditure for St Thomas More.

8.2.1.2. Impact on the performance of your job or role (this matter is between each individual member of staff and their respective line manager and not a judgement to be made by any other member of staff.)

8.2.1.3. Break the law.

8.2.1.4. Bring St Thomas More into disrepute.

8.2.1.5. Detrimentally affect the performance of the school network by using large amounts of bandwidth whilst downloading or streaming music/video.

8.2.1.6. Impact on the availability or accessibility of resources on the school network for business use.

8.2.1.7. Any information contained with the school's network in any form is for use by the employees and volunteers within the school for the duration of their period of work and should not be used in any way other than for the running of the school and the delivery of teaching within the school and none of the school's data should leave the site or be transferred onto any other format.

9. Portable and Mobile ICT Equipment

9.1. This section covers items such as laptops, mobile devices and removable data storage devices, please refer to paragraph 7 of this document when considering storing or transferring personal, identifying or sensitive data.

9.2. Use of any portable and mobile ICT equipment must be authorized by your Interm IT Consultant before use. This includes mobile phones, personal iPads or Android devices ect.

9.3. All activities carried out on the St Thomas More network and hardware will be monitored in accordance with the specifications laid out within this policy and staff will be held accountable should any of these breach any policy statements.

9.4. Employees and volunteers must ensure that all data belonging to the school is stored on the central network and not kept solely on the C: drive of a laptop or main drive of another device. Any equipment where any personally identifying data is likely to be stored **MUST** be encrypted. This is entirely non-negotiable.

9.5. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car for example, equipment and hardware managed by the school should be locked securely in the boot of the vehicle and not on show in the main compartment of the vehicle. Any hardware damaged or stolen when off of the school site, is not covered by insurance and therefore staff may be personally liable for repair or replacement costs.

9.6. Ensure portable and mobile ICT equipment is made available as necessary for antivirus updates, software installations, patches, upgrades and policy compliance checks as and when requested by the relevant staff.

9.7. Regardless of device, installation of any applications or software packages is strictly forbidden

9.8. In areas where any of the aforementioned device are likely to be around members of the general public, the equipment must not be let unattended and where possible, must be kept out of sight.

9.9. Portable equipment must be transported in a protective case/bag if one is supplied.

9.10. Laptops and mobile devices must have appropriate access protection, i.e. strong passwords and relevant encryption and as previously mentioned, should not be left unattended in public places.

9.11. Avoid writing down or otherwise recording any network access information where possible. Any information that is recorded physically, must be kept in a secure location and otherwise disguised so that no other person, member of staff or otherwise is able to identify what that information relates to.

9.12. Protect St Thomas More's information and data at all times, including any materials printed whilst on-site. This includes the destruction of any sheets of paper containing any personal or identifying information.

9.13. Users of laptops or mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged whilst not on-site. Appropriate precautions should be taken to minimize both the threat of theft and damage.

9.14. Care should be taken when working on any devices in public places (e.g. trains) to ensure that no school data or details are visible to members of the general public or anyone other than the user of that specific device.

10. Remote Access

10.1. Every member of the teaching and administration staff has full access to the Remote Desktop Server, when working remotely, from home or elsewhere.

10.2. Specific geo-blocking has been enabled on the Remote Desktop Server, preventing members of staff from accessing the Remote Desktop Server when they are out of the country, this has been enabled to prevent any form of Brute Force attack from a foreign nation and is designed to protect the school and it's data and not hinder its staff.

10.3. Instructions for access and use for the Remote Desktop Server are available from the school office and from your Interm IT Consultant.

10.4. Any and all use of the RDS is to be within all of the following and aforementioned policy statements and any use of the RDS that breaches **ANY** of the following or previous statements, will be subject to disciplinary action.

11. Electronic and Remote Monitoring

11.1. Through management of the broader school network, the Head teacher and the school's designated Interm IT Consultant have access and permissions to access electronic information about users on the network. As a part of their support of the school network, Interm IT have remote access to ALL devices on site and they are viewable and accessible at any time during the working day when they are turned on and in use. This access is only utilized when the school request support for

something specific and remote access is arranged, however, the tool that performs the monitoring (**Senso**) works on a machine learning/automated basis 24 hours a day, 7 days a week. Throughout the school year and all designated holidays.

In the case of a specific allegation of misconduct, a number of tools will be used, including **Senso**, to obtain evidence of these allegations and can/will be used as evidence or proof of any claim of misconduct in an official investigation. Within **Senso**, from time to time, it will flag keywords in potentially sensitive information or documentation and anything flagged within **Senso** and then seen by your support technician or partners is bound by confidentiality. This documentation may be viewed or seen when Interm IT cannot avoid accessing such information whilst fixing a problem but this will only be carried out with the consent of the individual(s) concerned.

12. Online Purchasing

12.1. Any users (who in their lunch, break or planning time) place and pay for any orders online using personal details do so at their own risk and Forres school accepts no liability if details are fraudulently obtained whilst the user is using the school's network, software, wireless internet or equipment.

13. Care of Equipment

13.1. Do not under any circumstance rearrange or move the way in which any equipment is placed in a room or plugged in (computers, speakers, power supplies, phones, network cabling etc.) without first contacting and consulting with the appropriate member of staff (typically this would be your Interm IT Consultant.)

14. Agreement

14.1. All employees, volunteers, contractors and temporary employees who have been granted access to the school's network and physical hardware are required to sign this agreement confirming their understanding and acceptance of this policy and its specificities. Any members of school staff, volunteers, contractors ect who do NOT comply with this policy and all of its policy statements, forfeit their right to access the school K9 network and any/all of it's shared resources and any breach of this policy and it's contained statements can be considered grounds for disciplinary and potentially (pending an appropriate investigation) dismissal.