**St Thomas More Catholic Primary school, Saffron Walden**

# COMPUTING & DATA PROTECTION POLICY

Policy No. STM-002

| | |
|---|---|
| Unique Policy Reference No | ***STM-002*** |
| Approved by (inc date) | *Governing Body* |
| Date Version Approved | *02/04/2025* |
| Date next due for review | *March 2026* |
| Author *(Document Owner)* | *Headteacher* |

# COMPUTING & DATA PROTECTION POLICY

## 1. Introduction

1.1. Technology plays a vital role in education, enhancing learning and teaching across the curriculum. This policy ensures that all computing resources are used legally, securely, and effectively, safeguarding the school community.

1.2. This policy applies to all employees, volunteers, visitors, pu and any other users of computing equipment and digital resources on school premises.

## 2. Ownership and Responsibility

1.3. All computing equipment and information resources remain the property of St. Thomas More Catholic Primary School.

1.4. Users must:

a) Ensure compliance with legal and regulatory requirements, including the UK GDPR and Data Protection Act 2018.

b) Use resources responsibly and in the best interests of the school.

c) Maintain the security and integrity of school systems.

## 3. Disciplinary Measures

Serious breaches of this policy may result in disciplinary action, including dismissal. Misuse of computing facilities that impacts productivity, reputation, or security may lead to investigation under the school's Disciplinary Procedure Policy.

## 4. Security

4.1. Users are responsible for activities conducted under their login credentials.

4.2. Passwords must not be shared; any compromise must be reported immediately.

4.3. Unattended computers must be locked to prevent unauthorised access.

4.4. Use of external USB or hard drives should be avoided unless encrypted and approved by IT support.

4.5. Unauthorised access to systems is a criminal offence under the Computer Misuse Act 1990.

## 5. Use of Email and Internet

5.1. Email should be used for school-related communication.

5.2. Confidential information must not be sent externally without appropriate encryption.

5.3. Users must not send or store indecent, discriminatory, offensive, or copyrighted materials.

5.4. Personal opinions shared via email must be clearly stated as such.

5.5. Accessing or sharing inappropriate online content is strictly prohibited.

5.6. The school reserves the right to monitor electronic communications under the Regulation of Investigatory Powers Act 2000.

## 6. Social Media and Personal Use

6.1. Social media use during working hours must be restricted to school-related purposes.

6.2. Staff must not post content that could damage the school's reputation.

6.3. Personal accounts must not list the school as an employer or disclose confidential information.

6.4. The school monitors online activity for policy compliance.

## 7. Data Protection and Confidentiality

7.1. All personal and sensitive data must be stored securely and accessed only when necessary.

7.2. Encryption must be used when transmitting confidential information.

7.3. Users must verify recipients before sending sensitive information.

7.4. Printed confidential materials must be securely disposed of.

7.5. Data breaches must be reported immediately to the Data Protection Officer (DPO) [Katie Harris, gdpr@intermit.co.uk, UK GDPR Practitioner and Data Protection Officer]

## 8. Remote Access and Portable Devices

8.1. Staff must access school resources remotely only via the approved Remote Desktop Server (RDS).

8.2. School-issued devices must be encrypted and stored securely.

8.3. Personal devices must not store or access school data.

8.4. Lost or stolen devices must be reported immediately.

## 9. Electronic Monitoring

9.1. The school uses monitoring tools such as Senso Safeguarding to ensure compliance.

9.2. IT support staff have remote access for maintenance but must maintain confidentiality.

9.3. Any misuse detected through monitoring may result in disciplinary action.

## 10. Use of School ICT Facilities

10.1. Personal use of school facilities is allowed within reason but must not interfere with work duties.

10.2. Streaming or downloading non-educational content is prohibited.

10.3. Users must not install unapproved software.

10.4. Any damage to school equipment must be reported.

## 11. Agreement and Compliance

All staff, volunteers, and contractors must sign an agreement confirming their understanding and acceptance of this policy. Failure to comply may result in the loss of access to school systems and disciplinary action.

For any queries regarding this policy, contact the **Headteacher** or the **Data Protection Officer**.