St Thérèse of Lisieux
Catholic Multi Academy Trust

IT Acceptable Use Policy

Audience:	**All Staff**
Approved:	**Board – 19/10/21**
Other related policies:	**Data Protection and Freedom of Information Policy, Records Management Policy**
Policy Owner:	**James McGeachie – Chief Executive Officer**
Policy Model:	**Compliance – all CMAT Academies use this policy**
Review:	**Annually**
Version Number:	**1.2 (September 2021)**

What you may and may not do when you use the St Thérèse of Lisieux CMAT IT systems and resources, and the consequences of breaking the rules.

Introduction

It is the responsibility of all users of Trust IT resources to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.1 Purpose

This Acceptable Use Policy is intended to provide a framework for such use. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

1.2 Scope

Members of the Trust and all other users (staff, students, visitors, contractors and others) of our facilities are bound by the provisions of this Acceptable Use Policy. The St Thérèse of Lisieux CMAT seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of the Central Team's services to the academies in the Trust, and therefore in turn supporting learning and teaching to the highest possible standards.

2 Unacceptable Use

a) IT resources may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

1. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3. unsolicited "nuisance" emails;
4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the Academy or a third party;
5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
6. material with the intent to defraud or which is likely to deceive a third party;
7. material which advocates or promotes any unlawful act;
8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
9. material that brings the Trust into disrepute.

b) The Trust resources must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

1. intentionally wasting staff effort or other Trust resources;
2. corrupting, altering or destroying another User's data without their consent;
3. disrupting the work of other Users

c) Users shall not intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

3 Data Protection Compliance

a) Users should ensure data protection compliance, and suitable measures should be taken to prevent a data breach including but not limited to:

1. All computers should be accessed by a password, including a mixture of upper and lower case letters and numbers. This password should be changed regularly.
2. Never write down or share passwords.
3. Always lock your computer when leaving your desk.
4. Work laptops and mobile phones should be encrypted with a password.
5. Do not use USB sticks or other storage devices unless they are encrypted and password protected.
6. Encrypted, password protected devices with up-to-date antivirus software may be used whilst working from home and to access work email accounts. CMAT documents must be accessed and saved in the cloud, such as One Drive, and must not be saved to a personal device.
7. Do not leave sensitive information on printers. Ideally printers should be accessed via a password – ensure you log out when leaving the printer.
8. Password protect all sensitive email attachments. Provide the password by phone or separate email. Do not include sensitive information in the main body of an email.
9. Encrypt sensitive emails.
10. Use pseudonyms when required to protect personal data.
11. Ensure extra precautions are taken when processing/sending sensitive information.

4 Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a User the Trust may in its sole discretion:

a) restrict or terminate a User's right to use the IT resources;

b) withdraw or remove any material uploaded by that User in contravention of this Policy; or

c) where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

d) in addition the Trust may take such action, disciplinary or otherwise as it deems appropriate in accordance with the Trust's policies.

Sign: _____ Date: _____

Print: _____