Acceptable Use Agreement

Staff and Volunteers

ST CLARE
Catholic Multi Academy Trust

Adopted by St Clare Trust Board;

Next review by St Clare Trust Board;

St Clare Catholic Multi Academy Trust Acceptable Use Agreement for Staff and Volunteers

This Acceptable Use Policy is intended to ensure that trust IT and communication systems are used in a safe way and are kept operational for the benefit of all in the trust community.

This agreement applies any time you use any systems provided by the trust, whether on trust premises or remotely and from any device, trust owned or personal.

Trust IT systems are designed to support teaching and learning, systems should primarily be used for study, teaching, or administrative purposes. The trust allows for modest personal use of trust systems providing the terms of this policy are not breached and that personal use is not detrimental to your duties.

Acceptable Use Policy Agreement

Trust systems in general:

- At all times your use of trust IT systems will be consistent with the values and ethos of the trust.
- A professional standard of communication is expected at all times both online and off line.
- Use of trust systems must be consistent with all other trust policies including those on Data Protection, Social Media and the Dignity and Mutual Respect Policy. You must read and understand these.
- Do not disclose your username or password to anyone else, or try to use any other person's username and password. If someone else knows your password change it immediately and notify IT Support staff.
- You must not use the trust systems to conduct any form of commercial activity without the express permission of the CFO.
- You may not use any form of virtual private network or file sharing software unless authorised to do so.
- You may not install any software or attempt to run any software from any other source without the express approval of IT Support staff.

Monitoring:

- Trust systems are monitored and filtered for the safety of all users. You must not attempt to circumvent any monitoring and your usage can be reviewed at any time.

Communication:

- Some email can contain malicious links or code, please be vigilant for suspicious email and if you unsure check with IT Support staff before opening any email or link that you are suspicious of.
- Trust provided e-mail accounts may be accessed by other members of staff as deemed appropriate to ensure smooth running of the trust. Access is at the discretion of a member of SMT or the IT Support staff, for example for the purposes of business continuity where a member of staff is absent through illness.
- You must only communicate with students and parents and carers using official trust systems.

Using your own device:

- You may only connect your personal device (smartphone / tablet / laptop etc.) to the designated wireless network of the trust and only when suitable credentials are provided by the trust. You must not connect any device directly to the physical network cabling of the trust. Any use of any trust systems (even via your own device) is filtered and monitored.
- You must not store any personal data relating to the trust, its staff or pupils, including images on personal devices, even if only temporarily. The only exception to this is that you may synchronise trust mail to a personal mobile device providing that device is solely used by you and is protected by either a fingerprint or other method of locking. You must not synchronise mail to a shared device of any sort, e.g. family computer or shared tablet.
- You must not sync Trust Onedrive / Google Drives to personal devices.
- You may only use any password manager feature (eg password manager software or the password manager feature of some web browsers) to store trust passwords if the device you are using is personal to you (not shared by any other family member) and is protected by a locking password or other security feature such as a fingerprint.

Data Protection:

- You must only transport, hold, disclose or share personal information about yourself or others, as outlined in the trust's Data Protection Policy (or other relevant policy). You must not transfer data from trust systems without the express permission of the trust Data Protection Officer, unless it is covered by policy documentation. All transfers of personal data must be encrypted to prevent inadvertent data loss.
- The trust data protection policy requires that any staff or student data to which you have access, will be kept private and confidential, except when it is deemed necessary that you are required by law or by trust policy to disclose such information to an appropriate authority.
- If you become aware of a data breach, potential or actual, you have a duty to report it to the data protection officer as soon as you become aware of the breach.

Acceptable Use Policy Agreement

I have read and understand the Staff and Volunteer Acceptable Use Policy and I agree to use Trust systems according to this policy.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to action under the Trust's disciplinary policy, and in the event of illegal activities, the involvement of the police.

Name:	
Signed:	
Date:	