

**Acceptable Use Policy for
IT/Social Media/Electronic Communications/Mobile
Phones/Laptops/Portable Devices**

Document Owner	IT
Last updated	June 2025
Version number	4

Policy Contents

	Page Number(s)
1. Application of this Policy	3
2. Relationship with DEMAT Values	3
3. Associated Policies and Documents	3
4. Version Control	4
5. Acceptable use policy for Trust employees	4-6

1. Application of this Policy

The policy is applicable to all employees (permanent and temporary) of DEMAT. Where applicable, it is also applicable to all Volunteers supporting DEMAT.

The above definitions are included for reference purposes for both School and Central Team staff to enable clarity and transparency when applying this policy.

2. Relationship with our Values

The application of this policy must be applied at all times in a way that reflects the values of DEMAT:

Love – We engender love and tolerance between and for our staff, pupils and others to foster an inspiring atmosphere of mutual support.

Community – We are committed to ensuring our schools are a living part of the community and contribute positively to its needs.

Respect – We do everything to provide a caring, safe and secure place for our staff and pupils to be happy and respected in our schools so they may achieve their potential.

Trust – We acknowledge accountability and responsibility for our actions and ensure that we encourage each other to make brave decisions and then learn from any mistakes.

Ambition – We are determined that our schools offer a place for the joy of learning, enabling those of all abilities to thrive and go on to lead rewarding lives.

This is further defined in the four key strands of DEMAT, all of which are underpinned by our Christian distinctiveness,

Children are at the heart of all we do

Keep close to the work

Maintaining a legacy, creating new traditions

Aspirational, yet sustainable

3. Associated Policies and Documents

This Policy/Procedure should be read in conjunction with the following DEMAT Policies/Procedures:

- **Code of Conduct**

4. Version control

No.	Status of document/changes	Prepared by	Reviewed by	Approved by	Date of approval
1.	Version 4 – Amends Staff are required to use multi-factor authentication / two factor authentication for all systems used in DEMAT, where it is available.	IT	HR	CEO	June 2025
2.	Personal mobile phones are allowed to be used for accessing multi factor / two factor authentication apps when required for work related systems. Personal mobile phones should not be used in classrooms for any other purposes.				

5. Acceptable Use of IT for Staff

This document will be reviewed on an annual basis. For all questions in relation to this policy, please contact IT on itsupport@demat.org.uk

This policy outlines acceptable of IT software, internet, email, social media, via laptops, PCs, tablets, mobile phones and other portable devices. It has a focus on all employees working across the Trust.

The purpose is to ensure safe and acceptable use of technology for the use of communication and delivering education or support for education alongside personal use of the above. It lists the responsibilities that all staff must ensure that any form of communication using technology is used appropriately and in line with GDPR rules.

The Trust/schools will try to ensure that everyone has good access to IT to enhance their role and to be able to provide the relevant learning opportunities for pupils.

All employees must understand that the Trust/schools will monitor the use of ICT systems including email and other digital communications.

Trust employees must ensure that they take responsibility for reading and upholding the standards laid out in this policy, and that:

- All technological devices have password/encryption facilities installed (for mobiles this must be a minimum of a 4-digit passcode).
- Staff are required to use multi-factor authentication / two factor authentication for all systems used in DEMAT, where it is available.
- PC/laptop or other equipment remains locked when unattended to ensure unauthorised access is prevented.

- Passwords must not be shared or disclosed to others and staff will not attempt to gain access to other passwords or devices.
- Passwords should not be written down and kept where they may be accessed. Passwords are not stored for sites within browsers, e.g. Internet Explorer/Chrome, etc.
- If there are concerns about receiving an unexpected email, staff contact the person by telephone before opening it, to ensure its credibility. If they are advised it was not sent by that person, they must contact their IT support team and DEMAT DPO for IT to investigate and keep the DPO updated on the outcome(s).
- Any form of hardware or software should not be inappropriately stored on any Trust-owned device without the Trust's permission or Headteachers permission (delegated to the headteacher, if school-based).
- Staff use a Trust or school email address for any correspondence that they send in relation to their role in the Trust/school.
- Any emails with attachments that contain personal or sensitive data are encrypted with a password. Password must be sent to the recipient using another transport method or are saved onto a secure shared site, and a secure link is provided that is only accessible by the designated recipient.
- When replying to personal email addresses the reply does not include attachments that contain personal data. Attachments containing personal data must always be sent via a Trust email addresses, with any attachments encrypted.
- Staff respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services is unacceptable.
- All data is kept secure and used appropriately as authorised by the Trust (delegated to the headteacher if school based).
- There is awareness of where any Trust/school-owned devices are at all times. All devices are stored securely when not in use. Laptops/mobile devices that are taken off-site must be stored securely out of sight. If left in a vehicle they must not be in view but stored securely in the boot with the vehicle locked.
- Staff do not use/duplicate/remove or amend anyone else's documents without their prior permission.
- There must be no downloading, copying, or distributing anything protected by copyright.
- Professional boundaries are maintained when using the internet and social media for personal use. When posting on personal forums/social media staff must ensure that they understand that the use of any comments or photos, regardless of whether they are positive or negative, can be shared with others (parents, pupils, colleagues) and this could lead to losing control of who sees them, or a misinterpretation of what was written: this could then bring your professional role and workplace into disrepute.

- Staff do not participate in communicating with pupils/parents outside of their role at the Trust when using work or personal technology/devices for the use of social media, texting, calling, etc. It is important to ensure that a professional relationship is always maintained to prevent any misinterpretation of any actions made.
- No personal details are exchanged with pupils that would allow contact directly via personal email, telephone or address.
- All communications with pupils must be via the Trust's/school's internal network.
- Trust/school equipment is not used to up- or download any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography, etc, covered by the Obscene Publications Act) or anything that is inappropriate or may cause harm or distress to others.
- No device is used for bullying, harassment or discrimination of others, in any form.
- The use of Trust/school equipment to access personal sites (social media) is not acceptable.
- Personal mobile phones are allowed to be used for accessing multi factor / two factor authentication apps when required for work related systems. Personal mobile phones should not be used in classrooms for any other purposes.
- Any incidents of concern regarding social media misuse are reported immediately to the relevant line manager. This includes but is not limited to illegal, inappropriate or harmful material.
- If any work device is stolen (laptop/mobile phone/iPad or similar), it must be reported to the Trust's Data Protection Officer (DPO) **immediately** as this is considered a breach under GDPR, and the DPO will need to report it within 72 hours.
- There is a commitment to being responsible users, at all times. Any misuse or failure to comply with this policy could result in disciplinary action. The Trust's HR function and the DPO must be notified of any misuse. Any safeguarding concerns will be reported to LADO and in the event of illegal activity the Trust will ensure third party involvement which may include the police.