Acceptable Use Policy for Trust Employees in the use of IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices

In the development of this policy consideration has been given to Equality and Diversity and Data Protection.

Equality and Diversity

The Diocese of Ely Multi-Academy Trust (DEMAT) is committed to promoting equality of opportunity for all staff and job applicants. The Trust aims to create a supportive and inclusive working environment in which all individuals are able to make best use of their skills, free from discrimination or harassment, and in which all decisions are based on merit. We do not discriminate against staff on the basis of age; race; sex; disability; sexual orientation; gender reassignment; marriage and civil partnership; pregnancy and maternity; religion, faith or belief (Equality Act 2010 protected characteristics). The principles of non-discrimination and equality of opportunity also apply to the way in which staff and Governors treat visitors, volunteers, contractors and former staff members.

Data Protection

DEMAT will process personal data of staff (which may be held on paper, electronically, or otherwise). DEMAT recognises the need to treat this data in an appropriate and lawful manner, in accordance with the Data Protection Act 2018 (DPA).

This policy is to be used across all of DEMAT and its schools	Version	Date
DEMAT Officer responsible for updating content: DPO	4	June 2020
Date approved by DEMAT Standards & Ethos Committee	2	Sept 2018
Effective date as determined by DEMAT	2	1 Sept 2018
Policy to be reviewed annually from date last approved by DEMAT Standards & Ethos Committee	4 (no procedural changes)	Annually
Policy review by DEMAT (no statutory revisions required as at June 2020)	4	June 2020
Policy to be reviewed by DEMAT (unless statutory revisions require it be done earlier)	4	June 2021

Policy Contents

Application of the Policy

This policy is to be used by all employees employed by The Diocese of Ely Multi-Academy Trust (DEMAT).

Acceptable Use Policy for Trust Employees

In using technology for the use of communication for education and personal use, including but not limited to: IT software, internet, email, social media, via laptops, PCs, tablets, mobile phones and other portable devices

This acceptable use policy is for all Trust employees, to ensure safe and acceptable use of technology for the use of communication for education and personal use, including but not limited to: IT software, internet, email, social media, via laptops, PCs, tablets, mobile phones and other mobile devices, and lists the responsibilities they have in ensuring any form of communication using technology that they use in their role 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.

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).
- They lock their PC/laptop or other equipment when leaving it unattended to ensure unauthorised access is prevented.
- They do not disclose or share any passwords provided for their use to others and will not attempt to gain access to anyone else's passwords. Passwords will not be written down and kept where anyone else can gain access to them.
- They do not store passwords for sites within browsers, eg Internet Explorer/Chrome etc. See **Appendix A**.
- If they think they may have received an unexpected email, they 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). This is following several schools across the UK receiving a number of malware emails.
- They do not install any hardware or software on any Trust-owned device without the Trust's permission (delegated to the headteacher if school based).
- They are using 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 or are saved onto a secure shared site, giving the link to where it can be accessed.
- When replying to personal email addresses, no attachments that contain personal data are sent. Attachments containing personal data must always be sent via a business email address, with any attachments encrypted.

The Diocese of Ely Multi Academy Trust (DEMAT)
Grace Building, 8 High Street, Ely, Cambridgeshire. CB7 4JU Tel: 01353 656760
Company registration number: 08464996

- They 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).
- They know where any Trust/school-owned device is at all times and they are responsible for ensuring it is securely stored when not in use (this is for any item that is allocated to them for use in their role). Laptops/mobile devices that are taken off-site must be stored securely out of sight. If left in a vehicle they must not be left in view but stored in the boot and the vehicle locked.
- They do not download apps to enable access to work emails/files on their personal devices. Access to emails/files must only be accessed through a web browser, but they must ensure that they log out each time they access it. If the only means of calling the emergency services to an incident is by using a personal mobile phone, that is automatically approved.
- They do not use/duplicate/remove or amend anyone else's documents without their prior permission.
- They do not download, copy or distribute anything that is protected by copyright.
- They maintain professional boundaries when using the internet and social media for personal use. When posting on personal forums/social media they 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.
- They 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 maintained at all times 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.
- They do not use Trust/school equipment 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 or harassment of others in any form.
- The use of Trust/school equipment to access personal sites (social media) is not used unless they are on a break and not in an area that affects others nearby.
- Personal mobile phones are not used in schools where children are present. Mobile phones should be locked away during school hours but can be used when on a break away from pupils.
- They report any incidents of concern regarding social media misuse to their line manager in the first instance. This includes but is not limited to illegal, inappropriate or harmful material.

- If any work device (laptop/mobile phone/iPad or similar) is stolen, 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.
- They agree to be responsible users at all times, they understand that they are responsible for their actions, and that misuse or failure to comply with this policy could result in disciplinary action of a verbal and/or written warning, suspension, and the involvement of the police in the event of illegal activity. The Trust's HR function and the DPO must be notified of any misuse.

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

All employees are asked to sign and date the following form to confirm they have received a copy of this Acceptable Use Policy, and have read and agree to abide by it.

Agreement to abide by the Acceptable Use Policy for Trust Employees in the use of IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices

I confirm that I have received a copy of the above policy, and have read it. I understand that I must comply with the above policy and understand that any breach could result in disciplinary action.

I will **immediately** report the loss of any equipment covered by this policy to the DPO at dpo@demat.org.uk.

I will report any incidents of concern regarding misuse of technology/software/social media to my line manager in the first instance.

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

Name: _____

Signed: _____

Position: _____

Location _____

(School name or DEMAT office):

Date: _____

Appendix A

Acceptable Use Policy for all users in the use of: IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices

How to change your Office 365 Password:

1) Sign in to your Office 365 account
2) Go to **Settings** > **Office 365 settings** > **Password** > **Change password**
3) Type your old password, and then type a new password and confirm it
4) Click **Submit**

How to Remove a Saved Password from a browser

If you store passwords for regularly accessed web addresses (eg Pupil Asset, etc), these saved password lists can expose the data it protects to anyone else who uses your computer, and possibly to others on the Internet, particularly if your device is 'hacked'. DEMAT therefore asks you not to store these passwords. If you already have stored passwords, below are a few ways to delete them, depending on the web browser you use:

Internet Explorer

To delete individual passwords:

1. Open Internet Explorer
2. Select ⋮ top right corner (the three vertical dots)
3. Choose Settings (towards bottom of list)
4. Choose Advanced Settings
5. Choose Manage Passwords
6. Click each web address and choose (**remove/delete**) until all gone

To prevent being prompted to save passwords, make sure the slide button under Passwords is in the OFF position.

Chrome

To delete individual passwords:

1. Open Chrome
2. Select ⋮ top right corner (the three vertical dots)
3. Choose Settings (towards bottom of list)
4. Choose Passwords
5. Click each web address and choose **remove** until all gone

To prevent being prompted to save passwords, make sure the slide button opposite Offer to Save Passwords is in the OFF position.