Acceptable Use – ICT Policy

Document control			
Approved by	Full Trustees	Approved date	14 September 2023
Next Review	September 2024	Policy Level	Non statutory
Published	Intranet and website		

Version	*Date issued*	*Author*	*Update information*
V1.0	12/12/2017	N McDermott	First published version
V1.1	19/12/2019	N McDermott	Minor updates to aid reading ease. 2.6 Addition of potential charge for damage.
V1.2	22/10/2020	N McDermott	Update of 2.7 to reflect Trust's monitoring and filtering solution. Addition of 3.14 to reflect Homeworking.
V1.3	06/09/2022	M Butler	Update to title of policy to Acceptable Use ICT – Staff. 2.6 reworded to include rolling 12-month period for repairs and 3.8 included with regards to the use of USB sticks.
V1.4	18/8/2023	M Butler	Reviewed. No changes required

Contents

1. Introduction

1.1. As a professional organisation with responsibility for safeguarding, all staff within the Dartmoor Multi Academy Trust are expected to take all possible and necessary measures to protect personal data and information systems and devices from damage, loss, unauthorised access, infection, abuse and theft.

1.2. We will ensure that all members of our community are safe and responsible uses of technology. We will support our staff to:

- Become empowered and responsible digital creators and users.
- Use resources and technology safely, carefully and responsibly, respecting system security and password security.
- Be safe and considerate online and create a community that is respectful and caring, on and offline.

1.3. All members of staff have a responsibility to use the Trust's computer systems in a professional, lawful, and ethical manner, consistent with the Trust's ethos, national/local guidance and expectations, the law, and relevant Trust and school policies including:

- Employee Code of Conduct
- Social Media Policy
- Personal Devices (Mobile Phones) Policy
- Data Protection Policy

- Safeguarding Policy / Keeping Children Safe in Education
- Online Safety Policy

1.4. This policy should be read in conjunction with the Acceptable Use Policy for Pupils. Those principles apply equally in this policy.

1.5. This policy forms part of the terms and conditions set out in the contract of employment.

2. System security

2.1. Hardware and software provided by the workplace for staff use can only be used by members of staff and only for educational use. Personal accounts or information such as personal photographs, files or financial information should not be accessed or stored on school devices and the Trust accepts no liability for loss of such data.

2.2. Downloading or accessing programmes or files that have not been authorised by IT system managers could result in the activation of malware or ransomware when devices are reconnected to school networks. If in doubt, staff should ask their IT support for guidance. Where there is a resultant data breach, staff may be individually liable for such a breach.

2.3. Staff must not remove or attempt to inhibit any software placed on school devices that is required by the school for network compliance or security.

2.4. Staff must not attempt to bypass any filtering and/or security systems put in place by the school.

2.5. Damage or loss of a computer, system or data including physical damage, viruses or other malware must be reported to the school's ICT support as soon as possible.

2.6. Staff are liable for any loss, theft or damage to equipment whilst it is in their care. Staff may be charged for any such damage unless it can be attributed to reasonable wear and tear. A maximum of three repairs without charge will be carried out for a user within a 12-month rolling period. Any loss of equipment will be charged to the user at cost to the Trust. The Trust can provide details of the value of the equipment for any personal insurance purposes.

2.7. The Trust reserves the right to monitor the activity of users on school systems and school devices from time to time. This includes real-time, digital monitoring of both keystrokes and screen views of harmful content and filtered access to restricted internet sites.

2.8. Password security is important. Get Safe Online provides guidance on password security and recommended Do's and Don'ts https://www.getsafeonline.org/protecting-yourself/passwords/

2.9. Equipment remains the property of the school. The school may request the return of any equipment for any reason at any time by giving appropriate notice. If you leave the employment of the school, staff must return equipment prior to the leaving date.

3. Data protection

3.1. Staff must be aware of their responsibilities under Data Protection legislation (including GDPR) regarding personal data of pupils, staff or parents/carers. This means that all personal data must be obtained and processed fairly and lawfully, kept only for specific purposes, held no longer than necessary and kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed

remotely. This includes safe and secure back up.

3.2. Staff should seek to use designated school software such as Arbor, CPOMS, or other proprietary software to store, manage, process or view personal information wherever possible to ensure security of information, appropriate deletion and archiving, and to ensure that searches in response to Subject Access Requests can easily and readily be completed.

3.3. E-mails created or received as part of your School job may be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or a Subject Access Request under the Data Protection Act 2018. All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper. Avoid using pupil/ staff names in email headers. All electronic communications with pupils, parents, outside agencies and staff must be compatible with the professional role of staff. The person about whom an email relates may request copies of the information therein.

3.4. Staff are reminded that any sharing of data with third parties should be subject to scrutiny by the school's Data Protection Lead to ensure an appropriate GDPR compliant data sharing agreement and appropriate licensing are in force.

3.5. Staff must not keep school-related personal information, including sensitive information, images, files, videos or emails, on any non-school issued devices.

3.6. Staff should use appropriate school platforms (such as Office 365 or GSuite) to access work documents and files in a password protected environment.

3.7. Any data being removed from the school site (such as via email) must be suitably protected. This may include email/ data being encrypted by a method approved by the school.

3.8. Staff are not permitted to use USB sticks unless approval has been granted by the Digital Team for technical reasons and such devices are encrypted.

3.9. Any images or videos of pupils must only be for official school use and reflect parental consent. Staff should ensure photos and videos are regularly uploaded to a shared network or official cloud drive, regularly deleted in line with retention policies, and removed from standalone devices such as iPads.

3.10. Staff are expected to respect copyright and intellectual property rights.

3.11. Staff must use school provided email accounts for all official communication, to minimise unsolicited or malicious email and to ensure all personal data is processed securely. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business. Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

3.12. Staff should actively manage e-mail accounts, delete e-mails of short-term value and carry out frequent housekeeping on all folders and archives.

3.13. Emailing personal, sensitive, confidential or classified information should be sent using appropriate secure email services, such as Egress to a named recipient, with Delivered/ Read receipt, or other secure delivery services such as S2S.

3.14. Staff must be mindful of their duties under Data Protection when working from home and should be familiar with the Trust's Homeworking Policy available on the Trust's website https://www.dartmoormat.org.uk/policies-and-documents.html .

4. Safeguarding

4.1. Staff are expected to immediately report any illegal, inappropriate or harmful material or incidents they become aware of, to the Designated Safeguarding Lead.

4.2. Queries or questions regarding safe and professional practice online either in school or off site should be raised with the Designated Safeguarding Lead or the Head teacher.

5. Appendix 1: Equipment Loan Agreement

This agreement covers short and long term loan of school/college equipment. The term 'equipment' refers to any electronic device and/or non-electronic apparatus.

By signing this agreement, you agree to abide by the terms and conditions set out above.

You are responsible for transferring or backing up any files/data you have created and stored within its internal memory/ hard drive. School/College staff cannot accept responsibility for the loss of data stored in this way, or data which are lost or erased during repair or reconfiguration.

I agree to the above conditions:

Equipment Type	
Make and Model	
Asset No.	
Signature (staff)	
Print Name	
Date Returned	
Received in good condition Y/N	
Signed (IT support)	