

IT Staff Acceptable Use Policy (including mobile phones and cameras)

Policy Monitoring, Evaluation and Review

This policy is effective for all schools within The Mead Educational Trust, the Teaching School, the SCITT and all other activities under the control of the Trust and reporting to the Trust Board. Employees not based in a school

Version:	6.1
Date created:	August 2018
Last updated:	January 2024
Author:	Debbie Stanley
Ratified by:	Executive Team
Date ratified:	January 2024
Review date:	January 2025

Revision History:

Version	Date	Author	Summary of Changes:
1.0	August 2018	DST	New policy
2.0	February 2019	DST	Added new clause under Section 4.3. about use of personal mobile devices
3.0	June 2019 Aug 2020	CJO EMA	Added additional dauses under Section 4.3. about use of personal mobile devices Amended review date to coincide with Online Safety Policy.
4.0	January 2021	GSM MPR	Added additional dauses under 4.2 about use of doud storage
5.0	January 2022	GSM	Additional dause 4.3.9 about never leaving devices in a vehicle overnight. Reinstatement of text from dause 4.6.7 which had been deleted in V4.0. Addional dause 4.3.18 regarding software installation on school owned devices.
6.0	February 2022	MPR	Amendments to dause 4.3.16 around staff use of personal mobile devices whilst students are present.
6.0	January 2023	GSM	Policy reviewed and no further changes
6.1	January 2024	GSM	Changed references to academy to school

Contents

1	Introduction	3
2	Scope and purpose	3
	Monitoring	
	Policy rules	
	Review of policy	

1 Introduction

- 1.1 ICT is provided to support and improve the teaching and learning in the Trust as well as ensuring the smooth operation of our administrative and financial systems.
- 1.2 This policy sets out our expectations in relation to the use of any computer or other electronic device on our network, including how ICT should be used and accessed within the Trust.
- 1.3 The policy links to the Trust Social Media Policy which provides advice and guidance to our employees on the safe use of social media. The acceptable use of ICT will be covered during induction and ongoing training will be provided, as appropriate.
- 1.4 This policy has been agreed following consultation with the recognised trade unions. It has been formally adopted by the Board.
- 1.5 This policy does not form part of any employee's contract of employment and may be amended at any time, however a breach of this policy is likely to result in disciplinary action.

2 Scope and purpose

- 2.1 This policy applies to all employees and temporary users (supply staff, governors, trustees, volunteers, visitors and contractors) using our ICT facilities. Ensuring ICT is used correctly, and that inappropriate use is avoided is the responsibility of every employee. If you are unsure about any matter or issue relating to this policy you should speak to your line manager, the network manager or a senior member of staff.
- 2.2 The purpose of this policy is to ensure that all employees are clear on the rules and their obligations when using ICT to protect the Trust and its employees from risk.
- 2.3 Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.
- 2.4 Any failure to comply with this policy may be managed through the disciplinary procedure. If we are required to investigate a breach of this

network manager or a senior manager.

- 4.2 The network and appropriate use of equipment
 - 4.2.1 You are permitted to adjust computer settings for comfort and ease of use.
 - 4.2.2 Computer hardware has been provided for use by employees and pupils and is positioned in specific areas. If there is a problem with any equipment or you feel it would be better sited in another position to suit your needs, please contact your line manager.
 - 4.2.3 Do not disclose your login username and password to anyone (unless directed to do so by a senior manager for monitoring purposes or as stated in dause 2.4).
 - 4.2.4 You are required to change your password in accordance with the login prompts. Ensure that you create appropriate passwords as directed. Do not write passwords down where they could be used by another individual.
 - 4.2.5 Do not allow pupils to access or use your personal logon rights to any system, Pupils are not permitted these access rights as it could lead to a breach of GDPR and network security. Allowing pupils such access could put you at risk if your accounts are used.
 - 4.2.6 Before leaving a computer for any length of time, you must log off the network or lock the computer, checking that the logging off procedure is complete before you leave.
 - 4.2.7 Ensure projectors linked to the network are switched off when not in use.
 - 4.2.8 Only software provided by the network may be run on TMET computers and laptops. You are not permitted to import or download applications or games from the internet unless IT agrees to do this on your behalf.
 - 4.2.9 You must not use any removable storage devices, such as USB pens where you are unsure of the content or origin.

- school insurance cover and the member of staff may be liable for the cost of a replacement.
- 4.3.9 Mobile devices must NEVER be left in a vehicle overnight.
- 4.3.10 At home, mobile devices must be stored securely.
- 4.3.11 The school/Trust cannot accept responsibility for any damage caused to mobile devices or their contents (files, folders etc.) by neglect or inappropriate use. In these circumstances, the school/Trust reserves the right to recover part/full costs from the employee.
- 4.3.12 The school/Trust cannot accept responsibility for any loss of a mobile device where it is deemed that this loss occurred as a result of neglect. In these circumstances, the school/Trust reserves the right to recover part/full costs from the employee.
- 4.3.13 Mobile devices not provided by us must have up to date anti-virus installed before being connected to the network.
- 4.3.14 You must ensure you have the appropriate permissions and security in place in order to access our network at home.
- 4.3.15 Accessing work resources and systems on personal devices, with the appropriate device security, is permitted. We reserve the right to apply data protection policies to any device that access data owned by the Trust, schools and departments (for example, Office 365).
- 4.3.16 Staff must not have their mobile phones on display or use for any purpose including

4.4.8 No personal device must ever be used to photograph children.

4.5 Internet safety

- 4.5.1 Never give out personal information such as your address, telephone number or mobile number over the internet without being sure that the receiver is from a reputable source.
- 4.5.2 Never give out personal information about a pupil or another employee over the internet without being sure that the request is valid and you have the permission to do so.
- 4.5.3 Always alert the Network Manager or Principal if you view content that makes you feel uncomfortable or you think is unsuitable. Remember that any personal accounts accessed on our network will be subject to monitoring.
- 4.5.4 Always alert the Network Manager or Principal if you receive any messages that make you feel uncomfortable or you think are unsuitable.
- 4.5.5 Alert the Network Manager or Principal if you receive Phishing, malicious or alarming content that may or may not cause a data breach to our network.
- 4.5.6 Abide by the guidance on links received in emails and other communication platforms. Do not enter any personal or login information through any links that were not expected.

4.6 Internet and email

- 4.6.1 The internet and email facilities are provided to support the aims and objective of the Trust. Both should be used with care and responsibility.
- 4.6.2 Use of the internet at work must not interfere with the efficient performance of your role. We reserve the right to remove internet access to any employee at work.
- 4.6.3 You must only access those services you have been given permission to use.
- 4.6.4 Before sending an email, you should check it carefully and consider whether the content is appropriate. You should treat emails like you would any other form of formal written communication.

4.6.5

Non-educational games Gambling

- 4.6.10 Do not send malicious or inappropriate pictures of children or young people including pupils, or any pornographic images through any email facility. If you are involved in these activities the matter will be referred to the LADO and the police.
- 4.6.11 Under no circumstances should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or young people. This material includes, but is not limited to pornography, unethical or illegal requests, racism, sexis

ICT Acceptable Use Policy for employees/temporary users

Employee/temporary user (print name):

Employee/temporary user Agreement:

I have read and

Staff Acceptable Use Policy.

I will use the computer network, internet and other technologies in are sponsible way in accordance with the rules set out in the policy.

I understand that network, systems and internet access may be monitored.