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

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 should substitute 'Principal' with CEO or appropriate representative.

Version:	6.2
Last review:	January 2025
Ratified by:	Executive Team
Date ratified:	21st January 2025
Next review:	September 2025 (annual review)

Revision History:

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

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 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, academy councillors, trustees, volunteers, visitors and contractors) using our ICT facilities.

2.2 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.

2.3 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.

2.4 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.

2.5 Any failure to comply with this policy may be managed through the disciplinary procedure. If we are required to investigate a breach of this policy, you will be required to share relevant password and login details.

2.6 If you reasonably believe that a colleague has breached this policy, you should report it without delay to your line manager or a senior member of staff.

3. Monitoring

3.1 The contents of our ICT resources and communications systems are our property. Therefore, employees should have no expectation of privacy in any message, files, data, document, facsimile, social media post, blog, conversation or message, or any other kind of information or communication transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems. Do not use our ICT resources and communications systems for any matter that you wish to be kept private or confidential.

3.2 We reserve the right to monitor, intercept and review employee activities using our ICT resources and communications systems, to ensure that our rules are being complied with and are being used for legitimate business purposes.

3.3 We may store copies of data or communications accessed as part of monitoring for a period of time after they are created, and in doing so will comply with GDPR.

4. Policy rules

4.1 In using the Trust's ICT resources, the following rules should be adhered to. For advice and guidance on these rules and how to ensure compliance with them, you should contact the 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.

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/interactive screens 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.

4.2.10 Pupil or staff data, or any other confidential information should not be stored on a memory stick and should only be stored on encrypted devices and not taken off the premises unless it has been encrypted to ensure data protection and confidentiality.

4.2.11 Removable Storage Devices should only be used for Trust purposes, outside of our premises where they are encrypted or have appropriate password protections. The use of cloud-based storage, such as OneDrive is recommended as an alternative.

4.2.12 Approved Cloud Storage options should only be used to store Trust, school and confidential data (such as OneDrive). The use of other Cloud Storage providers for storage of material owned by the Trust/Schools is prohibited.

4.3 Mobile devices and laptop use

The following rules are for use of any laptop, electronic tablets, mobile phone or other mobile device including those provided by the Trust. Referred to as mobile device(s):

4.3.1 If you choose to use your own mobile device for school business, you do so at your own risk and must ensure compliance with this policy and the GDPR policy if using any data or network.

4.3.2 While use of Trust email addresses on mobile devices is permitted, the processing of any personal data is prohibited e.g. processing personal data through text, personal email, and social messaging apps.

4.3.3 Access to our wireless network must be approved by the network manager or Principal.

4.3.4 You must ensure that any mobile device is password protected. This is essential if you are taking the mobile off our premises.

4.3.5 The employee is responsible for any loaned equipment and will take all necessary steps to keep the items secure and free from risk of damage.

4.3.6 Any damage to devices, whether accidental or otherwise, should be reported to IT Support as soon as possible.

4.3.7 Whilst in transit, mobile devices must be stored out of sight, preferably in the boot of the car. If the car is left unattended briefly and you need to leave the mobile device in the car then it MUST be stored in the boot, out of sight. Failure to do so will negate the school insurance cover and the member of staff may be liable for the cost of a replacement.

4.3.8 Mobile devices must NEVER be left in a vehicle overnight.

4.3.9 At home, mobile devices must be stored securely.

4.3.10 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.

4.3.11 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.

4.3.12 Mobile devices not provided by TMET must have up to date anti-virus installed before being connected to the network.

4.3.13 You must ensure you have the appropriate permissions and security in place in order to access our network at home.

4.3.14 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).

4.3.15 Staff must not have their mobile phones on display or use for any purpose including emailing, texting, making calls, receiving calls whilst pupils are present. This protects staff against any allegation made towards them. If for any reason staff need to use their mobile device for an educational purpose/activity they must seek written permission from their line manager. Use of personal mobile devices must be restricted to non-contact time, and to areas of the school where pupils are not present (such as a staff room). There may be circumstances in which it's appropriate for a member of staff to have use of their mobile device during contact time e.g. for emergency contact by their child/their child's school or in the case of acutely ill dependents or family members. In such cases, staff members must seek written permission from the Principal to allow for special arrangements in advance. If special arrangements are not deemed necessary, staff can use the school office number as a point of emergency contact.

4.3.16 Staff must not use their mobile devices to take photographs or recordings of pupils or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

4.3.17 Mobile devices remain the property of the school/Trust and software must be authorised by IT prior to installation. Restrictions are in place for such scenarios.

4.4 Cameras

4.4.1 Photographs may only be taken and used for any purpose if consent has been given and consent must be in the form of a completed consent form.

4.4.2 It is essential that photographs are taken and stored appropriately to safeguard the children in our care.

4.4.3 Only designated cameras provided by the school are to be used to take any photos of children.

4.4.4 Images taken on the designated camera(s) must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.

4.4.5 All staff are responsible for the security of the cameras when assigned.

4.4.6 Images taken and stored on the camera must be downloaded in school as soon as possible, ideally once a week by IT.

4.4.7 Under no circumstances must cameras of any kind be taken into the toilet area whilst pupils are or may be present.

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 Although the email system is provided for business purposes, we understand that employees may on occasion need to send or receive personal emails using their work email address. This should be kept to a minimum and should not affect, or be to the detriment of, you carrying out your role effectively. When sending personal emails from your work email account you should show the same care in terms of content as when sending work-related emails.

4.6.6 The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be considered under the disciplinary procedure.

4.6.7 You should not send electronic messages which are impolite, use obscene language, are indecent, abusive, discriminating, racist, homophobic or in any way intended to make the recipient feel uncomfortable. This will be considered under the disciplinary procedure.

4.6.8 If you receive an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, you should not forward it to any other address but you should alert the Principal or your line manager.

4.6.9 Do not access any sites which may contain inappropriate material or facilities, including but not limited to:

- Proxy
- Dating
- Hacking software
- Pornographic content
- Malicious content
- Music downloads
- 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, sexism, homophobia, inappropriate language, or any use which may be likely to cause offence. If you are not sure about this, or come across any such materials, you must inform the Principal or a senior manager.

4.6.12 Do not upload or download unauthorised software and attempt to run on a networked computer; in particular hacking software, encryption and virus software.

4.6.13 Do not use the computer network to gain unauthorised access to any other computer network.

4.6.14 Do not attempt to spread viruses.

4.6.15 Do not transmit material subject to copyright or which is protected by trade secret which is forbidden by law.

4.6.16 Never open attachments of files if you are unsure of their origin; delete these files or report to the network manager or senior manager.

4.6.17 Do not download, use or upload any material from the internet, unless you have the owner's permission.

4.7 The following acts are prohibited in relation to the use of the ICT systems and will not be tolerated:

4.7.1 Violating copyright laws

4.7.2 Attempting to harm minors in any way

4.7.3 Impersonation of any person or entity, or to falsely state or otherwise misrepresent an affiliation with a person or entity

4.7.4 Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service

4.7.5 Uploading, posting, messaging or otherwise transmitting any content that without the right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements)

4.7.6 Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party

4.7.7 Uploading, posting, messaging or otherwise transmitting any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of solicitation.

4.7.8 "Stalking" or otherwise harassing any user or employee.

4.7.9 Collection or storage of personal data about other users

If you are in any doubt about this policy in practice, please speak to your line manager or the Principal before acting.