



Equipment Loan Policy (inc. Mobile Phones)

Document date: July 2022



Together, pursuing life in all its fullness

Version	Date	Author	Changes
v1.0	06/02/2019	Jo Baker/Louise Beale	Adapted from Mobile Phone policy to incorporate all loan equipment
v2.0	August 2019	Louise Beale	Forms extracted from policy
V3.0	July 2022	Louise Beale	Reviewed and sections re-ordered

Review frequency	3 years
Review date	July 2025
Ratified by	Trust Leadership Team
Date of ratification	18.07.2022
Lead/owner	Head of Operation and Compliance
Target audience	All staff
Document reference	POL-HR09

The electronic version is the definitive version of this document.

CONTENTS

- 1. The Purpose of the Policy**
- 2. The Use of Trust Issued Equipment**
- 3. Lost or Stolen Equipment**
- 4. Use of a Device Whilst Driving**
- 5. Trust Laptop / Tablet or Chromebook etc**
- 6. Trust Issued Mobile Phones**
 - 6.1 The Use of Trust Issued Mobile Phones
 - 6.2 Monitoring of Usage and Costs
 - 6.3 Pool Phones
 - 6.4 Mobile Phone Use Abroad
- 7. Keys/Entry Fobs**
- 8. Appendix – Forms**

1. THE PURPOSE OF THE POLCY

- 1.1. Equipment is issued to staff to assist with the effective operation of the academy and the Multi Academy Trust and the academies within it (the Trust). The issue of equipment is to facilitate staff in their roles and, as such the Trust have certain expectations regarding the use of Trust equipment. The aim of this policy is to clearly outline the protocols for issue and use of trust equipment.
- 1.2. It is the responsibility of the Headteacher and Academy/Cluster Business Manager/Partner to ensure that all relevant staff members issued with Trust equipment are aware of, and understand this policy and any subsequent revision.
- 1.3. Every member of staff issued with Trust equipment must sign the Agreement (appendix A or Appendix B)

2. THE USE OF TRUST ISSUED EQUIPMENT

- 2.1 Where equipment has been issued by the Trust, it is for **business use only** and at all times will remain the property of the Trust. The user(s) will be responsible for its safekeeping, proper use, condition and eventual return to the Trust. The Trust reserves the right to recover the cost of any repair or replacement where damage, other than fair wear and tear, has occurred to the equipment. If a replacement is required the Trust will organise this.
- 2.2 Only applications appropriate to the user's work should be downloaded onto a device. Any unapproved apps that incur additional costs will be passed to the end user. The Trust reserves the right to deduct those costs, either through deduction from pay or otherwise and may, after formal investigation, take action under the Disciplinary Procedure.
- 2.3 The user is ultimately liable for the misuse of Trust equipment. The user should not access, store or distribute any offensive or inappropriate material using a device or equipment. The Trust may, after formal investigation, take action under the Disciplinary Procedure in such cases.
- 2.4 The user agrees that upon termination of employment, should they not return the allocated equipment, or should the equipment be returned in an unsatisfactory condition, the cost of replacement, or a proportional amount of this as decided by the Trust, will be deducted from any final monies owing, or the user will otherwise reimburse the Trust.
- 2.5 The user is ultimately liable for the misuse of a Trust device. The user should not access, store or distribute any offensive or inappropriate material using the device. The Trust may, after formal investigation, take action under the Disciplinary Procedure in such cases.

3.0 LOST OR STOLEN EQUIPMENT

3.1 The user is responsible at all times for the security of the equipment and the data stored on it. Where the user has access to Office 365 no data should be held on the device. If data is stored on a device the data must be encrypted. The equipment should never be left unattended.

3.2 The highest levels of security should be set to protect unauthorised access to a device. As a minimum a security PIN code should be set on the device. The security PIN code should not be shared with other people (in the case of pool phones this will only be shared with authorised users of the pool phone)..

3.3 The line manager must be informed of the theft or loss as soon as practicably possible, who will report it accordingly to the Head of Operations and Compliance who may need to inform the Head of Finance and/or the Data Protection Officer and in the case of mobile phones, O2 on 0344 809 0202 as soon as possible to ensure that the account is stopped and there is no unauthorised usage.

3.4 In the event of theft of a laptop or mobile phone, the incident must also be reported to the police and an incident number obtained (please provide this number when reporting the loss to the line manager).

3.5 The Multi Academy Trust reserves the right to claim reimbursement for the cost of the equipment if:

- the correct procedures have not been followed,
- a user reports repeated loss of their equipment,
- it is deemed that the user has not taken appropriate measures to safeguard the equipment,
- the user has not reported the loss in a timely manner.

4.0 USE OF A DEVICE WHILST DRIVING

4.1 The user must ensure they have full control of any vehicle that they are driving at all times and any devices must be operated in accordance with the law, including not using a handheld device whilst driving or whilst the engine is turned on.

4.2 Individuals are personally responsible for the payment of any fine or fixed penalty incurred whilst in charge of a vehicle. Any conviction for driving offences, any driving endorsements and any fines incurred whilst driving a vehicle belonging to the Trust must be reported immediately to the Head of Operations and Compliance as this may affect the Multi Academy Trust's insurance.

4.3 It should be noted carefully that a breach of the Trust's rules on the use of a mobile phone whilst driving may render the user liable to action under the Disciplinary Procedure.

5.0 TRUST LAPTOP, TABLET OR CHROMEBOOK ETC

5.1 As a borrower of a Trust laptop / tablet or chromebook etc, you accept the following responsibilities:

- To follow the guidelines established in any Acceptable use policy for ICT / E Safety Agreement / Data Security Policy.
- To follow the guidelines listed below for proper care of the equipment.
- To use the computer for school or professional development purposes.
- Not to write on or place any labels or stickers on the equipment.
- Not to disable or uninstall any safety and security applications such as virus protection and firewalls that are provided with the equipment.
- To store data on the Trust Office 365 account or if there is no access to Office 365, to ensure any documents created are securely stored and moved from the device to the Trust network as soon as possible.
- To bring the device to work daily, when at work and log in to the network to ensure that antivirus software and other updates pushed out through the network are current.
- To report any problems/issued encountered while using the device to the line manager.
- To allow IT staff to reimage the device at any point where it becomes unusable or unstable and at the end of the year.
- Understand that reimaging may be a course of action for any repairs or modifications on the computer and this will result in the loss of all data from the laptop.
- Only make any modifications in the computer's settings for usability or accessibility reasons only.
- To return all devices at the end of the school year for inventory and software updates as required. Devices may be reassigned as deemed appropriate by the administration.

5.2 Proper care is to be given to the device at all times, including but not limited to the following:

- Other individuals, including children, should not be allowed to play on the computer.
- Care appropriate for any electrical device.
- Use a surge protector or unplug the laptop during electrical storms.
- Keep food and drink away from the computer.
- Do not leave the device exposed to direct sunlight or extreme cold.
- Position the device on a safe surface so it does not drop or fall.
- Do not attempt to repair a damaged or malfunctioning device.
- Do not attempt to upgrade the computer or software.

5.3 Proper security is to be provided for the device at all times, including, but not limited to, the following:

- Secure your device in a safe place at the end of the day.
- Do not leave the device in an unlocked car.
- A device left in a locked car must be out of sight, for example in the boot.
- Do not leave the A/C adapter behind when moving the device.
- Ensure the device is secured with password protection and/or encryption.

6.0 TRUST ISSUED MOBILE PHONES

6.1 THE USE OF TRUST ISSUED MOBILE PHONES

6.1.1. Users should not sign up to text based information services, e.g. RAC traffic alerts, text voting. Smartphone users should only use the internet to access their work emails and for other Trust use.

6.1.2. The SIM card from Trust mobiles should not be placed into any other device, unless placed into another Trust issued mobile phone.

6.1.3. When using the camera function all images should be taken in line with the Trust policy for photographing images of children and these should be downloaded on to a secure area of the Trust IT systems and deleted from the phone as soon as possible. Photos or video should not be stored on the device unnecessarily.

6.1.4. The Trust recognises that users may, on occasion, have to make personal calls or send personal text messages during working hours, or outside normal working hours. Where it is deemed that an unreasonable amount of personal calls/text messages have been made using the mobile phone, the Trust reserves the right to deduct those costs, either through deduction from pay, or otherwise. The Trust may, after formal investigation, take action under the Disciplinary Procedure if such use is excessive or unauthorised. Users will be expected to make payment for private calls made beyond reasonable usage.

6.2 MONITORING OF USAGE AND COSTS

6.2.1 The Trust receives itemised billing for all Trust mobile phones and this is monitored on a monthly basis. The billing system identifies all calls, texts and data usage (if appropriate) and the costs related to this, by user, destination, duration, frequency, etc. High or clear personal usage will be reported to the line manager for investigation (high usage is defined as usage which falls outside of the normal usage pattern for the individual or outside of the usage pattern in comparison to other similar users).

6.2.2 This monitoring will allow the Trust to identify any areas of potential misuse or training that may be required, or to negotiate with suppliers any necessary changes in tariffs to ensure cost efficiency.

6.2.3 If it is found the mobile phone has been misused, the Trust may, after formal investigation, take action under the Disciplinary Procedure.

6.2.4 Mobile phones are issued to staff to aid in the operation of the daily working life. They should be kept charged, switched on and in possession of the member of staff during working hours unless where it would not be appropriate to have a phone switched on such as during a business meeting. If a user is not making use of the phone the Trust reserves the right to reallocate the phone to another member of staff.

6.3 POOL PHONES

- 6.3.1 Where a phone is not allocated to an individual but is shared by a number of users, it is the responsibility of the Academy/Cluster Business Manager/Partner to ensure that the phones are signed out to an individual and signed in when returned.
- 6.3.2 Each user must be given a copy of this policy and be given a clear understanding of the purpose and acceptable use that the phone is being issued for.
- 6.3.3 No confidential information, emails or personal data should be downloaded or stored on a pool phone. Any photographs or video taken should be downloaded on to a secure area of the Trust IT systems and deleted from the phone before returning the pool phone.

6.4 MOBILE PHONE USE ABROAD

- 6.4.1 Mobile phones issued by the Trust should not be used abroad unless the Head of Operations and Compliance has specifically given approval.
- 6.4.2 It is particularly important on Smartphones to ensure that “data roaming” is switched off when abroad. “Data roaming” charges from abroad (which includes the Isle of Man and Channel Islands) can result in very high level charges, and if it is found that these have been incurred due to personal use or negligence on the part of the user, then the charges may be passed on to the user.

7.0 KEYS / ENTRY FOBs

- 7.1 Key/fob holders must have due regard for the security of the academy and its facilities.
- 7.2 The keys to the academy buildings should only be held by an employee of the trust.
- 7.3 Where keys or entry fobs are provided to an employee a Staff receipt of Key Acknowledgement form (see Appendix B) must be completed and retained by the academy.
- 7.4 If a key or entry fob is lost the line manager must be notified immediately and the employee may be required to pay for new locks and their installation or duplicate keys to be cut as required.
- 7.5 No duplicates are to be cut without the prior permission of the Academy/Cluster Business Manager/Partner.

7.6 Any abuse of privilege such as entering the premises without permission, using the facilities or allowing other people or organisations to use the facilities without permission will result in the keys or entry fob being withdrawn and other action may be taken.

7.7 All keys or entry fobs must be handed back to the Academy/Cluster Business Manager/Partner when requested.

8.0 APPENDIX – FORMS

The following forms are located at Sharepoint/Info Hub/Forms, Policies and Templates/central Forms/HR:

- Loan of Academy / Multi Academy Trust Equipment
- Receipt of Key Acknowledgement Form