[01/09/2018]

Greater Manchester Academies Trust

Mobile Device Acceptable Use Policy

1. Mobile Device Acceptable Use Policy

1.1 Purpose

The purpose of this policy is to define standards, procedures, and restrictions for GMAT Staff who have legitimate educational uses for connecting mobile devices to GMAT's network and data. This mobile device policy applies, but is not limited to, all devices both personal and GMAT provided, and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablets
- E-readers
- Portable media devices
- Portable gaming devices
- Laptop/notebook/ultrabook computers
- Wearable computing devices
- Any other mobile device capable of storing corporate data and connecting to a network

In order to maintain security and manageability, only devices fitting the following criteria are allowed to access corporate resources:

- Smartphones, tablets, and other devices running Android version 7.0 (Nougat) and higher.
- Smartphones and tablets running iOS 10.11 (El Capitan) and higher.

The policy applies to any mobile hardware that is used to access GMAT resources, whether the device is owned by the user or by the organization.

The goal of this policy is to protect the confidentiality of staff, students, parents and supplier data that resides within GMAT's technology infrastructure, including internal and external cloud services.

This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unsanctioned resources.

A breach of this type could result in loss of information, none compliance with GDPR, damage to critical applications and to the GMAT's public image. Therefore, all users employing a mobile device connected to GMAT's network, and/or capable of backing up, storing, or otherwise accessing data of any type, must adhere to company-defined processes for doing so.

2. Applicability

This policy applies to all GMAT employees, including full and part-time staff, contractors, freelancers, and other agents who use a mobile device to access, store, back up, or relocate any GMAT data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust. Consequently, employment at GMAT does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

The policy addresses a range of threats to enterprise data, or related to its use, such as:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive corporate data is deliberately stolen and sold by an employee or unsanctioned third party.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced to or via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of GMAT's Data Protection Officer (DPO). **Non-sanctioned use of mobile devices to back up, store, and otherwise access any GMAT-related data is strictly forbidden.**

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the GMAT network.

2.1 Responsibilities

GMAT DPO has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

GMAT DPO has delegated the execution and maintenance of information technology and information systems to the GMAT IT Manager.

Other staff under the direction of the GMAT DPO are responsible for following the procedures and policies within information technology and information systems.

All GMAT employees are responsible to act in accordance with company policies and procedures.

2.2 Affected Technology

Connectivity of all GMAT provided mobile devices will be centrally managed by GMAT's IT department and will use authentication and strong encryption measures. Although IT will not directly manage personal devices purchased by employees, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. This means that any mobile device connecting to GAMT's infrastructure must have password authentication and device encryption. Failure to do so will result in immediate suspension of personal device network access privileges to protect GMAT's infrastructure.

3 Policy & Appropriate Use

It is the responsibility of any employee of GMAT who uses a mobile device to access resources to ensure that all security protocols normally used are adhered to. It is imperative that any mobile device that is used to conduct GMAT business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

3.1 Access Control

3.1.1. GMAT IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to GMAT's infrastructure. IT will engage in such action if such equipment is being used in a way that puts GMAT's systems, data, users, students and parents at risk.

3.1.2. Prior to initial use on the corporate network or related infrastructure, all mobile devices must be approved by GMAT IT. GMAT IT will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to corporate infrastructure. If your preferred device does not appear on this list, contact the help desk at itsupport@mca.manchester.sch.uk or 216. Although IT currently allows only listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in future.

3.1.3. End users who wish to connect such devices to GMAT's data must employ, for their devices and related infrastructure, security measures deemed necessary by GMAT IT. Enterprise data is not to be accessed on any hardware that fails to meet GMAT's established enterprise IT security standards.

3.1.4. All personal mobile devices attempting to connect to the GMAT network through the Internet will be inspected using technology centrally managed by GMAT's IT department. Devices that are not approved by GMAT IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect.

3.2 Mobile Device Management (MDM)

3.2.1. GMAT's IT department uses the Vodafone's mobile device management solution to secure mobile devices and enforce policies remotely. Before connecting a GMAT provided mobile device to network resources, the device must be set to be manageable by Vodafone's mobile device management system.

3.2.2. The mobile device management solution enables GMAT IT to take the following actions on mobile devices:

- Enable user authentication.
- Enforce consistent security policies.
- Encrypt sensitive corporate data.
- Manage user access to corporate resources.
- Establish network access controls.
- Separate corporate and personal data.
- Enforce compliance rules.
- Remotely wipe enterprise data from device and Apps.

3.2.3. Any attempt to contravene or bypass the mobile device management implementation will result in immediate disconnection from all corporate resources, and there may be additional consequences in accordance with GMAT's overarching security policy.

3.3 Security

3.3.1. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password; a PIN is not sufficient. All data stored on the device must be encrypted using strong encryption. See GMAT's password and encryption policy at [file location or URL] for additional background. Employees agree never to disclose their passwords to anyone.

3.3.2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.

3.3.3. Any non-corporate computers used to synchronize or back up data on mobile devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by GMAT's IT department.

3.3.4. Passwords and other confidential data, as defined by GMAT's IT department, are not to be stored unencrypted on mobile devices.

3.3.5. Any mobile device that is being used to store GMAT data must adhere to the authentication requirements of GMAT's IT department. In addition, all hardware security configurations must be pre-approved by GMAT's IT department before any enterprise data-carrying device can be connected to the corporate network.

3.3.6. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with GMAT's overarching security policy.

3.3.7. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once its use is no longer required.

3.3.8. In the event of a lost or stolen mobile device, it is the responsibility of the user to report the incident to GMAT IT immediately. If the device has been provided by GMAT, the device will be remotely wiped of all data and locked to prevent access by anyone other than GMAT IT. If the device is recovered, it can be submitted to IT for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to GMAT business or personal. The GMAT Remote Wipe Waiver, which ensures that the user understands that personal data may be erased in the rare event of a security breach, must be agreed to before connecting the device to corporate resources.

3.3.9. Usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.

3.3.10. Applications that have not been approved by GMAT IT and distributed through Vodafone's Mobile Device Management or deployed using Google's application push service, are not to be used within the workplace or in conjunction with GMAT data.

3.4 Hardware & Support

3.4.1. GMAT IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on GMAT's network.

3.4.2. Users will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, jailbreaking, rooting).

3.4.3. GMAT IT will support the connection of mobile devices to GMAT resources. On personally owned devices, IT will not support hardware issues or non-GMAT applications.

3.5 Organisational Protocol

3.5.1. GMAT IT can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to GMAT's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with GMAT's policies.

3.5.2. The end user agrees to immediately report to his/her manager and GMAT’s IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

3.5.3. Every mobile device user will be entitled and expected to attend a training session about this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

3.5.4. Any questions relating to this policy should be directed to GMAT’s IT Helpdesk, at 216 or itsupport@mca.manchester.sch.uk.

3.6 Policy Non-Compliance

Failure to comply with the *Mobile Device Acceptable Use Policy* may, at the full discretion of the organization, result in the **suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment**.

The (i) Data Protection Officer, (ii) Principal, and (iii) immediate line manager will be advised of breaches of this policy and will be responsible for appropriate remedial action.

3.7 Employee Declaration

I, [employee name], have read and understand the above *Mobile Device Acceptable Use Policy*, and consent to adhere to the rules outlined therein.

Employee Signature Date

Manager Signature Date

IT Administrator Signature Date