[01/09/2018]

Greater Manchester Academies Trust

Staff Information Acceptable Use Policy

Approved by:	A Woolley	**Date:**	[Date]11/09/2018
Last reviewed on:	[Date]		
Next review due by:	[01/09/2020		

Contents

Staff Information Acceptable Use Policy

1. Purpose

The internet and e-mail play an essential role in conducting GMAT businesses and services. The systems within GMAT are made available to students, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. GMAT values the ability to communicate with colleagues, pupils and business contacts, and needs to ensure that we always carry out these activities professionally and courteously at all times.

The purpose of this policy is to provide staff with clear guidance on the appropriate, safe, and legal way in which they can make use of information and IT equipment in GMAT. Staff need to be aware of the compliance required with this policy and technical measures taken to safeguard its data.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the GMAT IT Manager or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to HR.

2. Scope

2.1. This Acceptable Use Policy applies to you as an employee whatever your position, whether you are the Principal, Teacher, support staff, permanent, temporary or otherwise. Any inappropriate use of GMAT's internet, e-mail or application systems whether under this policy or otherwise may lead to disciplinary action being taken against you.

2.2. Other individuals and agencies who may gain access to data, such as volunteers, visiting professionals or researchers, and companies providing IT services to the Trust.

2.3. This policy covers the use of all GMAT IT systems, equipment and networks whether accessed on or off site. It applies to access gained through personal equipment being used on GMAT networks. In using these IT systems, equipment and network on or off GMAT facilities, implies acceptance of all terms and conditions within this and associated policies and of the consequences of inappropriate use.

3. Aim of this Policy

3.1. This document defines the GMAT portal, Internet and email Policy and:

3.1.1. sets out GMAT’s policy for the protection of the confidentiality, integrity and availability of the GMAT portal, Internet and e-mail system.

3.1.2. establishes GMAT’s and user’s responsibilities for the GMAT portal, Internet and e-mail system.

3.2. The objective of this policy is to ensure the security of GMAT IT system.

GMAT IT Team will:

3.2.3. ensure that the GMAT’s network, equipment and business applications is available to users.

3.2.4. protect the academy and its employees from activities that might expose them to legal action from other parties

3.2.5. protect the GMAT portal, Internet and email system from unauthorised or accidental modification ensuring the accuracy and completeness of GMAT's assets.

3.2.6. protect data assets against unauthorised disclosure.

4. General Principles and Legal Issues

4.1. GMAT IT Team will take all reasonable steps to ensure that users of GMAT's network resources and business applications are aware of acceptable use policies and legal obligations.

4.2. All information relating to our pupils, parents and staff is confidential. You must treat all GMAT information with the utmost care whether held on paper or electronically

4.3. Internet and e-mail access is intended to be used for GMAT business, educational services or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your line manager or Principal.

4.4. As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of GMAT where it is necessary for your duties. The processing of personal data is governed by the General Data Protection Act 2018.

4.5. All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

5. Computer Access Control

5.1. Access to GMAT IT systems is controlled by the use of user IDs and passwords. All user IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on IT systems and equipment by anyone who uses that ID. All those with a user ID must comply with the Password Management Policy.

Individuals must not:

5.1.1. Allow anyone else to use their user ID and password allocated to them on any GMAT system or equipment.

5.1.2. Leave their user accounts logged in at an unattended and unlocked computer.

5.1.3. Use someone else's user ID and password to access GMAT systems or equipment.

5.1.4. Leave their password unprotected (for example written down in view of others).

5.1.5. Perform any unauthorised changes to GMAT IT systems or information.

5.1.6. Gaining or attempting to gain unauthorised access to accounts or passwords

5.1.7. Respond to emails or anyone asking you to disclose your password. The GMAT IT Helpdesk will never ask you to divulge your password.

5.1.8. Providing evidence of business transactions; making sure the Trust's business procedures are adhered to; training and monitoring standards of service; preventing or detecting unauthorised use of the communications systems or criminal activities.

5.1.9. Maintaining the effective operation of communication systems.

6. Use of Internet

6.1. When entering an internet site, always read and comply with the terms and conditions governing its use.

6.2. Do not download any images, text or material which is copyright protected without the appropriate authorisation.

6.3. Do not download any images, text or material which is inappropriate or likely to cause offence.

6.4. If you are involved in creating, amending or deleting our web pages or content on our web sites, such actions should be consistent with your responsibilities and be in the best interests of GMAT.

6.5. You are expressly prohibited from:

6.5.1. using software that bypasses any security or filtering appliance;

6.5.2. seeking to gain access to restricted areas of the network;

6.5.3. knowingly seeking to access data which you are not authorised to view;

6.5.4. introducing any form of computer viruses;

6.5.5. carrying out other hacking activities.

6.5.6. for your information, the following activities are criminal offences under the Computer Misuse Act 1990:

6.5.7. unauthorized modification of computer material;

6.5.8. unauthorized access with intent to commit/facilitate the commission of further offences.

7. Use of Email

7.1. You should agree with recipients that the use of e-mail is an acceptable form of communication. Any material that is classed confidential, privileged, or sensitive should not be sent un-encrypted. It is good practice to indicate that the email is `Confidential@ in the subject line.

7.2. Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).

7.3. Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.

7.4. Sharing email account passwords with another person, or attempting to obtain another person's email account password. Email accounts are only to be used by the registered user.

7.5. Do not impersonate any other person when using e-mail or amend any messages received.

7.6. It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.

8. Social Media

8.1. GMAT permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

8.2. GMAT will take appropriate action in the event of breaches of this policy. Where conduct is found to be unacceptable, GMAT will deal with the matter internally. Where conduct is considered illegal, GMAT will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

8.3. Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of GMAT.

9. Data Protection

9.1. Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at GMAT's premises or working remotely you must:

9.1.1. keep the data private and confidential and you must not disclose information to any other person unless authorized to do so. If in doubt ask your line manager;

9.1.2. familiarize yourself with the General Data Protection Regulation Policy and comply with its provisions;

9.1.3. familiarize yourself with all appropriate GMAT policies and procedures;

9.1.4. not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information GMAT holds on them subject to any exemptions that may apply.

9.2. GMAT views any breach of the General Data Protection Regulation as gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures.

9.3. If you make or encourage another person to make an unauthorized disclosure knowingly or recklessly you may be held criminally liable.

9.4. Do not distribute confidential, privileged, sensitive or personal data unless you are using a secure site or portal.

10. Unacceptable Use

10.1. Install any software that is not provided by GMAT IT. To use pirated software or illegally use licensed software.

10.2. Modify or circumvent the precautions taken by GMAT IT to prevent virus infection.

10.3. Use the facilities for monetary gain

10.4. Prevent others from making legitimate, work related use of the facilities.

10.5. Try to gain unauthorised entry to other computer systems or files ('hacking').

10.6. Copy, delete or make changes to any files, directories or folders other than those in connection with their work.

10.7. Tamper, adjust, switch on/off or otherwise interfere with the equipment in open areas and teaching classrooms other than normal usage.

10.8. Transmission of unsolicited commercial or advertising material, save where that material is embedded within, or is otherwise part of, a service to which the recipient has chosen to subscribe

10.9. Creating, transmitting, transferring, downloading, browsing, viewing, reproducing or accessing any image, material or other data of any kind, which contains unacceptable content, including but not limited to:-

10.9.1. Sexually explicit messages, images, films, video clips, cartoons, jokes or any other material of a sexual nature

10.9.2. Any other content which may offend, harass, provoke, demean, degrade or threaten any other person (whether a fellow employee or a third party) whether on the grounds of

age, disability, gender re-assignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation

10.9.3. Any content that promotes violence, terrorism or extremism or contravenes current anti-terror legislation as per the Terrorism Act 2000 and UK Government Prevent Strategy 2011

10.9.4. Any content that is illegal, defamatory, malicious, libellous, derogatory or causes annoyance or needless anxiety

10.9.5. Any inappropriate use of social networks, chat-rooms, newsrooms, bulletin boards, blogs or wikis.

10.9.6. Any content that deliberately introduces a virus, malware or spyware into the GMAT network or systems or the network or systems of any other party, which is designed to corrupt or destroy the data of other users or in any other way compromise the integrity of those systems

10.9.7. Any content that infringes or may infringe the intellectual property or rights of others or data protection rights

10.9.8. Content that discloses information that is confidential to the University or its employees

10.9.9. Creation of content that benefits any political organization

10.9.10. Any content that may bring the University into disrepute.

10.9.11. Any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us).

10.9.12. Any content that breaches the UWS Policy on Dignity & Respect at Work.

11. Monitoring Communications

11.1. This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

11.1.1. to establish the existence of facts

11.1.2. to ascertain compliance with applicable regulatory or self regulatory practices or procedures.

11.1.3. to ascertain or demonstrate effective system operation technically and by users.

11.1.4. for national security/crime prevention or detection.

11.1.5. for confidential counselling/support services.

11.1.6. for Investigating or detecting unauthorized use of the system

11.1.7. for monitoring communications for the purpose of determining whether they are communications relevant to the business.

11.2. GMAT has an obligation to monitor the use of the internet and e-mail services provided in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. GMAT reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to send and receive electronic communications.

11.3. If the email is personal, it is good practice to use the word `personal' in the subject header and the footer text should indicate if it is a personal email GMAT does not accept responsibility for any agreement the user may be entering into.

11.4. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for GMAT's business purposes.

12. Declaration

I hereby confirm that I have read and fully understood the terms and conditions the Staff Information Use Policy and will strictly follow the policies of the usage of GMAT IT computing services.

Print Name: .....

Signature: .....

Date: .....