IT POLICY

Purpose

This policy covers the security and use of all of MMF's information and IT equipment, the use of email, the internet, voice and mobile equipment. This policy applies to all of MMF's employees, contractors and agents (hereafter referred to as 'individuals'). This policy applies to all information, in whatever form, relating to MMF's business activities and to all information handled by MMF relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by MMF or on its behalf.

MMF's IT Systems

- MMF staff are provided with access to a PC and/or laptop on the **Microsoft Azure** server with a **Microsoft Office 365** account for communications and file management.
- MMF uses **Speed Admin** software for managing and storing lesson data and customer communications.
- MMF uses **Microsoft Teams** for internal communications.
- MMF uses **Microsoft Sharepoint** and **OneDrive** for file storage/management.
- MMF recommends that staff access and send email via **Microsoft Outlook.**
- MMF uses the **Microsoft Office** suite for documents, spreadsheets and gathering data via online forms.
- MMF uses **Zoom** video communications for external teleconferencing and online teaching & learning (please refer to the Online Learning Policy).

Computer Access Control – Individual's Responsibility

Access to the MMF IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on MMF's IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any MMF IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access MMF's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to MMF's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-MMF authorised device to the MMF network or IT systems.
- Store MMF data on any non-authorised MMF equipment.
- Give or transfer MMF data or software to any person or organisation outside MMF without the authority of MMF.

Line managers should ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Password Policy

Individuals must ensure that all passwords used for MMF devices and systems are strong and kept secure. Any actual or suspected breach of an individual's password(s) must be reported to MMF leadership immediately.

Secure Passwords:

- Are long (minimum 16 characters)
- Are unique (cannot be used for any other service/system either personal or professional)
- Do not contain any personal information (e.g. date of birth, birth country etc)
- Contain a range of characters (uppercase, lowercase, symbols & numbers)
- Avoid using complete words or phrases

Compromised Passwords

MMF staff must change any passwords that they believe to have been compromised or that are known by someone else immediately and report to Senior Leadership / IT Administrator. To change your password, log in to Office 365 via a web browser and click on your account icon and then 'my account' - 'security info'. You will need to verify your identity via Multi-Factor Authentication.

Internet and email Conditions of Use

Use of MMF's internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to MMF in any way, not in breach of any term and condition of employment and does not place the individual or MMF in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which MMF considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to MMF, alter any information about it, or express any opinion about MMF, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward MMF mail to personal (non-MMF) email accounts.
- Make official commitments through the internet or email on behalf of MMF unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Lead / Support Organisation.
- Connect MMF devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, MMF enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example, password protecting confidential documents.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

File Storage and Management

To ensure MMF data and digital assets are accessible, individuals should follow the following file saving/naming conventions:

- All shared company files should be saved in the relevant location on Sharepoint (for most data this will be the 'General' channel).
- Files should be stored in the appropriate parent folder (e.g. 'Lessons', 'Schools' etc).
- Sub-folders should be used to organise parent folders (please check if the relevant sub-folder exists before creating one).
- Annually recurring/changing documents should be organised in further sub-folders by academic year ('2019-2020', '2020-2021' etc.).

Remote Working

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with MMF's remote working policies / subject to agreement from your line-manager
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- MMF equipment must not be used by non-MMF employees (e.g. family members)
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely. All data should be stored securely in the appropriate Sharepoint (e.g. 'General') or OneDrive location and not locally on the device.
- Reasonable care should be taken to avoid loss or damage of MMF laptops and mobile devices. Where reasonable preventative measures have been taken and loss or damage occurs (e.g. accidental damage), MMF will not hold the individual liable.

Bring your own Device (BYOD)

BYOD is restricted at Merton Music Foundation due to the security risk personal devices pose. You may not load MMF emails, Teams application, or files on your own personal computer, laptop, tablet, or mobile device, without prior written permission from management.

Mobile Devices

If you need to access emails on a mobile device, you will need to request permission from management. MMF operates a 'zero-trust' model for connecting phones to emails, so IT needs to first approve a phone before it receives emails. If a company phone or laptop is stolen it is your responsibility to notify management and Abbey Support immediately, as steps will need to be taken to protect against data theft.

If a mobile device is setup with access to MMF data, it must meet the following requirements:

- The mobile is kept updated to the latest operating system at all times.
- The Anti-virus application must never be disabled or uninstalled. If there is no anti-virus application, please install one from the Appstore. A recommended one is AVG anti-virus, but any application made by a well-known vendor is permissible.

- The mobile must have a password with a minimum of 8 characters. By default, mobiles 'throttle' the rate of attempts, meaning you must wait an increasing amount of time between unsuccessful login attempts.
- The mobile should lock itself after a period of inactivity, requiring the password to sign back in.
- The device must not be 'jailbroken', 'rooted' or had any of the manufacturers default security controls disabled.

Furthermore, MMF requires that:

- The device is not a shared device (e.g. family iPad).
- When not in use for business purposes, the device is logged-out of MMF systems.

NB: wherever possible, images, videos or recordings of pupils should not be made or stored on personal devices. Where this is necessary to support the organisation's media/marketing strategy, images must be transferred to MMF's data storage facilities on the same day and permanently deleted from the personal device and any related cloud-storage systems. Photo consent must be given in advance in accordance with data protection procedures. Employees must also refer to the procedures outlined in the Safeguarding Policy.

Software

Employees must use only software that is authorised by MMF on MMF's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on MMF computers must be approved and installed by the MMF IT Lead / Support Organisation.

Individuals must not store personal files such as music, video, photographs or games on MMF IT equipment, unless exception is granted by the system administrator.

Software Whitelist

The following software is whitelisted for use in the Foundation's IT network. Where users require access to software that is not listed below, written approval must be given by the Senior Leadership Team or IT admin and this list must be updated.

- Microsoft Office Suite (Word, Powerpoint etc)
- VLC Media Player
- Google Chrome
- Zoom
- WebEx
- Teams
- Zoom
- Audacity
- Zebra Badge Printer
- Badgy Badge Printer
- Dorico
- Sibelius
- MuseScore
- Exclaimer
- DYMO Label
- Skype
- TeamViewer

Viruses

MMF has implemented centralised, automated virus detection and virus software updates within its systems. All PCs have antivirus software installed to detect and remove any virus automatically. Individuals must not remove or disable anti-virus software or attempt to remove virus-infected files or clean up an infection, other than by the use of approved MMF anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of MMF voice equipment is intended for business use. Individuals must not use MMF's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- Use MMF's voice equipment for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

User Access and Privileges

All user accounts and associated privileges must be created following written approval of the Senior Leadership Team.

Where an employee changes role or responsibility within the organisation, their user privileges will be reviewed by the Senior Leadership Team and any changes to these will be made following written approval of the Senior Leadership Team.

Administrator Access

Administrator access is restricted to members of staff who are IT trained with responsibility for ensuring the safe and effective operation of MMF's IT systems.

Administrator privileges may only be granted by written approval of the Chief Executive and/or Operations Director.

Administrator accounts must not be used for day-to-day tasks, this is to mitigate the risk of these accounts becoming compromised. Users with administrative privileges require a secondary administrator account to their 'standard' account for day-to-day tasks such as email.

MMF grants administrator privileges to its IT support provider, Abbey Support, including remote access to user's desktops and external access to the Foundation's Draytek routers for remote administration and troubleshooting.

A record of all users with administrator access is maintained and the Senior Leadership Team review this quarterly.

User Account Review

IT administrators are responsible for reviewing all active user accounts quarterly to ensure that any unneeded or redundant accounts have been deactivated.

Actions upon Termination of Contract

All MMF equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to MMF at termination of contract. All MMF data or intellectual property developed or gained during the period of employment remains the property of MMF and must not be retained beyond termination or reused for any other purpose.

Upon the termination of contract, the following actions should be taken by IT Admin:

- The individual's Office 365 license should be downgraded to a basic license or unlicensed.
- The individual's Office 365 password is to be re-set and 'Block Sign-In' enabled.
- Auto-forwarding of incoming mail to be set up to go to a relevant member of the Senior Team.
- Auto-reply message created and enabled, giving suitable alternative contact information (e.g. admin@mmf.org.uk).
- The individual is to be removed from the Merton Music Foundation Team on Microsoft Teams.
- After an agreed period of time, suitable to the individual's former role in the organisation, the Office 365 account should be deleted.

Monitoring and Filtering

All data that is created and stored on MMF computers is the property of MMF and there is no official provision for individual data privacy, however wherever possible MMF will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. MMF has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 2018

It is your responsibility to report suspected breaches of security policy without delay to your line manager, the IT Lead, or the IT Support Organisation helpdesk.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with MMF disciplinary procedures.

UPDATED: Feb 2023

Appendix: How to Create a Secure Password

MMF staff are advised to make use of a password manager to facilitate the use of randomly generated secure passwords across all sites/devices. However, as the Office 365 password is also used to log-in to MMF devices, it needs to be memorable.

1. **Generate a list of completely random words that contain 5 letters or more**

   - Go to: https://randomwordgenerator.com/
   - For 'Number of Words' select – 10
   - Ignore 'Word Type' and 'First Letter' / 'Last Letter' – leave blank
   - For 'Word Size By' select 'Letters' and in the drop down 'Greater than'
   - Select '5' in the final box
   - Click 'Generate Random Words'

2. **Choose 3 or 4 of the words that are generated – pick words that stand out to you**

   - E.g: 'Qualification', 'Likely', 'Parade' (total number of characters = 25)
   - Or: 'Couple', 'Function', 'Direction'

   Tip – the sillier, the better as you are more likely to remember it!

3. **Combine the words into a long memorable phrase and then use add/remove letters, numbers, symbols & capitals to make the password more secure:**

   Tip: don't make common substitutions (e.g. '@' for 'a', '1' for 'i', or '£' for '3' etc)

   - E.G: qualificationlikelyparade = q2aliFcotianiKEl&par&£de
   - Or: couplefunctiondirection = (uPple7unc3ioN1ireC2ion

4. **Practise, practise, practise!**

   You may temporarily write the password down whilst you memorise it and practise using it. Log in and out of your laptop/email a few times – test yourself. Once you are confident, destroy the written copy.

5. **Never use this password for anything else.**

   This is very important – hackers rely on password re-use to gain access to your accounts using data breaches from other sites. This password can only ever be used for your MMF Office 365 account.

Re-Setting Your Office 365 Password:

You can re-set your password by logging in to Office 365, **click on your initials** in the top right-hand corner and selecting '**View Account**'. Next click '**Change Password**' (in the box labelled 'Password'). You may need to enter an authentication code which will be texted to your phone.

(NB: after re-setting your password, you will also need to re-login to OneDrive on your PC and enter your new email password on your phone if you use this to access MMF emails/calendar).