ACCEPTABLE USE POLICY

MGS-POL-IT-003

Policy Reference:	MGS-POL-IT-003	**Document author:**	Nima Mostoufi, Group Information Security & Compliance Officer
Version:	V3	**Approved By:**	Group Chief Information Security Officer
Issue date:	18/06/2025	**Next Review Due:**	18/06/2026
Document Scope:	All Group companies		

Issue, Review and Amendment

This Policy shall be made available through M Group Services intranets and its issue notified to relevant companies' employees through an internal memorandum or other appropriate form of communication.

An Appointed Person shall review this Policy at least once a year to re-affirm its conformity to the current requirements of company Policy or immediately if its contents are deemed to be no longer valid.

Where revisions are required, they shall be made by replacement of the applicable page(s). An amended revision number and the date of revision shall identify each revised document; this shall be detailed within the document revision table below.

When changes affect a considerable number of pages, this document shall be reissued/revised in its entirety, incorporating all previous revisions. A number shall identify issues and each issue shall cancel and replace all previous issues and revisions. Revisions shall be identified by a number and shall replace the previous revision.

Revisions shall be notified to relevant M Group Services companies' employees through an internal memorandum or other appropriate form of communication.

Document Reviews				
Date	Version	Author	Approved By	Changes
29/06/2020	v0.1	Ted Sefia		First document: Merge of Acceptable Use of (Data & Data Security, Internet & Email and Work Technology Equipment policies) and inclusion of s.9 Home Working.
21/07/2020	v0.2	Nick Scott		Reviewed and edited
21/07/2020	v1.0	Ted Sefia		Issued
22/09/2020	v1.0	Ted Sefia	Nick Scott	Update to s.3.7 and inclusion of s11.3
25/06/2021	v1.1	Ted Sefia	Nick Scott	Annual review, no change
25/06/2022	v1.2	Ted Sefia	Nick Scott	Update to s8 remote working

10/02/2023	v2.0	Ted Sefia	Nick Scott	Password, mobile and Teams update
19/01/2024	V2.1	Nima Mostoufi	Nick Scott	Minimum password character length updated in section 2.1 Updated police reporting link
04/6/2024	V2.2	Nima Mostoufi	Nick Scott	Password character length
				statement updated
18/6/2024	V2.3	Nima Mostoufi	Nick Scott	Addition of sections 3.8 and 3.9 (company devices and TVs)
18/6/2025	V3	Nima Mostoufi	CISO	Annual review Re-brand

Contents

1. Introduction

This policy provides guiding principles which stipulates the way in which M Group Services Companies' (referred to in this policy as Companies') networks, systems (including portable/mobile devices) and the internet may and can be used.

M Group companies operate a number of Information and Communications Technology (ICT) systems to support its business operations and the companies further provide the means for employees to use emails and the internet at work where appropriate. The companies' systems hold a variety of information including sensitive personal information and/or information that is protectively marked. Therefore, there is a requirement to place a premium on data security at all times.

Whilst systems are provided primarily for business use, occasional and reasonable personal use is permitted provided that this does not interfere with the performance of duties and is conducted during break times. Similarly, the use of email and the internet entails some risks and employees must follow the rules and security advice provided in this policy.

There is thus the need to impose controls on access to the internet and access to systems by users to protect the information held and to ensure that only authorised users who have a genuine need are allowed access. These rules are designed to minimise the risks to M Group Companies and any breach could lead to disciplinary action and may ultimately lead to dismissal. Where something is not specifically covered in this policy or an employee is unsure about whether something they propose to do may breach this policy, they should seek advice from their line manager.

Technology and the law change regularly, and this policy will be updated to account for changes as and when necessary. It is an employee's responsibility to be familiar with the latest version of this document.

1.1 Purpose

The purpose of this policy is to provide information to employees and authorised third parties on the rules in place for use of PC, the guidance on data security, password creation and protection, use of devices, emails, the internet, and social networking. It further provides guidance for remote users and homeworking and the use of removable media.

1.2 Scope

This policy applies to all users of M Group companies' IT assets and systems for email and internet. It also includes all users of the technological equipment and IT facilities supported by M Group Services companies. It covers all employees, agency staff, contractors, authorised third parties and customers. Failure to comply, or an unreasonable delay in compliance, constitutes a breach of this policy and may lead to disciplinary measures. Serious breaches of this policy will be regarded as gross misconduct and may result in immediate dismissal. The Police may be involved where there is suspicion of illegal activity.

This policy will be reviewed and updated to:

- Reflect changes in M Group data policies and procedures
- Add control statements that reflect industry best practice

2. PC and Data Security

When using laptops and handheld computers (HHC), the following guidance must be observed:

- Users should take appropriate security measures to protect the laptop/HHC and all its peripherals both inside and outside of the office
- Laptops/HHCs left on the companies' premises after work should be locked away out of sight in accordance with clear desk and environment policies.
- Laptops/HHCs must not be left in unsupervised areas.
- You must not leave your desk, a meeting or conference room without ensuring your laptop is secure.
- Laptops/HHCs used or kept at an employee's home address must be kept in a secure location and where possible locked away when unattended.
- When away from the office, laptops/HHCs should not be left unattended in view through a ground floor window.

To ensure information remains secure access to systems is prompted by entering your password and using Multi Factor Authentication (MFA).

2.1 Password Rules

Employees are required to set a strong password that meets with M Group Services guidelines and takes account of good practice. There may also be system specific rules that may be imposed on a case-by-case basis. The use of MFA may also be applied for certain applications or processes.

General guidance is as follows:

- You must not re-use any of the last 15 passwords
- You must change your password whenever prompted - typically this will be every 180 days. Accounts which do not have their passwords reset within the allocated time will become automatically locked out. Locked out accounts require unlocking by IT support staff.
- You cannot change your password multiple times on any given day
- Passwords have a minimum length of 12 characters (the previous minimum length of 8 characters is still valid and acceptable until we have applied the technical updates by October 2024)
- The password policy configuration for Group mobile devices managed via Intune is set to a minimum password length of 6 characters and history of 5
- Passwords must be "complex" and use "pass phrases" such as IDigHats..11 – a mix of upper and lower case, letters, numbers, and special characters (symbols allowed are @ # $ % ^ & * - _ ! + = [ ] { } | \ : ‘ , . ? / ` ~ “ ( ) ; < > blank space also allowed)
- You should use different passwords for different user credentials

2.2 Storing Passwords/ "Remember Me" Functionality

The companies' systems are configured to always require user credentials, and not to store passwords for future sessions. Features such as "Remember Me" should not be used to remember passwords. If prompted to do so this should be reported to the IT Service Desk.

2.3 Sharing Passwords

Passwords should not be shared. Employees are accountable for anything that is done on the companies' systems using their user credentials, including anything done by another person using their password.

If access to an employee's confidential files is required, for example, in their absence, the IT department can arrange for the files to be copied or moved to a location where they can be accessed. They should not be asked to disclose their password to a colleague for this purpose.

On occasions, it will be necessary to provide access to an employee's user-id, to enable IT support staff to make a change to their PC, for example. In these circumstances, it is the employee's responsibility to change their password once the required action is completed. If an employee is a new user and given user credentials that appear to relate to another user, this must be reported to the IT Service Desk

2.4 Compromised Passwords

If an employee is aware that passwords are being shared, or at least is known by others, they must:

- Notify the IT Service Desk – a password compromise is an Information Security event that must be properly recorded and investigated.

- Change the password immediately. If this is not possible, they must inform the IT Service Desk so that necessary measures can be taken to prevent the password being used by an unauthorised person.

2.5 Leaving a PC unattended

When leaving a PC or Laptop unattended for any period of time the employee must ensure that it cannot be accessed by anyone else by locking the screen. In addition, the employee should take all reasonable precautions to ensure that their laptop cannot be stolen, including, but not limited, to the following:

- Secure the Laptop when leaving the office for a period of time
- Never leave a laptop in open view in a public place or unattended vehicle
- When leaving a vehicle, the employee should either take the laptop with them or put it out of sight in the boot
- When at home the employee should make sure that the laptop is stored safely and out of public view
- Utilise security screens that reduce the chance of being overlooked.
- Any Laptop/PC that is lost or stolen should be reported to IT as soon as possible along with any associated references from the police (please follow information as provided in the reporting of theft or lost property from the British Police website here

2.6 Copying and Removing Data from a Company PC

Copying or removing data from any M Group Services companies' PC to a home PC which is not the property of the companies or emailing the companies' material to a home email address is not permitted. Any employee who needs access to the companies' information whilst not on site should ensure they are issued with the correct equipment by IT.

Employees with access to move data between locations should ensure that:

- Material that is protected under copyright by another person or institution is not copied or removed
- Company material is not to be copied or removed from the PC unless there is a legitimate and authorised business reason for doing so
- The companies' material is not to be shared with any third-party companies without authorisation
- The systems comply with data handling and classification policies.
- Any systems are fully encrypted

Any employee that believes they have contravened any of these points inadvertently, should inform their manager or the IT department immediately.

3. Work Technology Equipment Access

3.1 Access

Third party access to Companies' assets and Companies' access to third party assets:

The Companies' contracts that allow employees the use of third-party laptops must, as a minimum, comply with this policy and any further security controls mandated by the third party.

Where it is deemed appropriate and necessary for a third party to have access to the companies' laptop, this access must be risk assessed and authorised by the IT Department. Third parties must be made aware of the relevant M Group Services Information Security policies relating to the use of the Companies' assets and facilities. Laptop security procedures and confidentiality agreements between the Companies' and the third party must be documented.

3.2 During Travel

When travelling with laptops, the following guidance must be observed:

- Laptops should not be left unattended in public places, such as in luggage racks or whilst purchasing food/drinks or tickets.
- Whilst travelling in a vehicle, the laptop must not be visible by persons external to the vehicle when parked for any reason, including at service areas
- During air, rail, sea or coach travel, laptops must be kept as hand luggage. Under no circumstances must laptops be left unattended during a journey.
- Where employees are away from home staying in hotels, laptops must not be left in a car but taken into the hotel and kept in the hotel bedroom safe or stored in the hotel's secure facilities, where available.
- To minimise the risk of loss or theft, employees must risk assess the appropriateness and necessity to take their laptop when travelling on business.
- Care should be taken when using laptops in public places and on public transport to ensure sensitive information cannot be read.

3.3 Technical Protection

In order to protect information on laptops, employees should observe the following guidelines:

- Laptops must have encryption software installed to protect the information held within the device.
- When connecting remotely to the Companies' network, employees must use a secure connection (e.g., VPN). If you are in any doubt as to whether you have a secure connection, you must not connect remotely until you have confirmed this with the IT department.
- All laptop documents must be backed up to the Companies' network on a regular basis.

- Laptops must be connected to the Companies' network regularly, ideally as a minimum, on a weekly basis, to allow updates of security software and patches. In the event that this is not possible, due to absence from work (e.g., annual leave), users should ensure the laptop is updated at the earliest opportunity on returning to work. Users who do not connect to the Companies' network should ensure other suitable arrangements are agreed with the IT department.
- Employees must not use wireless connectivity to connect to any non-M Group Services companies' networks unless they are expressly authorised by their IT department and that it is conducted in accordance with their instructions.
- Laptops must be password protected in accordance with the password standard as provided in the policy.
- Personal data as defined in the Data Protection Act (2018) must not be stored on a laptop unless there is a pressing business need to do so. Where there is a need to store personal or sensitive data on a laptop then this must be authorised and monitored by management.
- Sensitive personal or the M Group company specific information stored on laptops should be minimised to lessen the aggregated risk if stolen/lost, but adequate for the user to perform their duties.
- The managers of remote workers should ensure that their employees' remote place(s) of work have adequate laptop security controls in line with the Companies' Information Security policies.

3.4 Personal Use

Personal use of laptops is subject to the restrictions contained within this policy and any other relevant M Group Services policies. In addition, employees should note that:

- Personal use of laptops is expected to be in a person's own time and is not to interfere with their job responsibilities or the job responsibilities of other employees.
- Employees must not attach personal equipment e.g., removable media, mobile phones, printers, cameras, scanners to a laptop without authorisation and guidance from the IT department.
- Employees must not allow unauthorised access to their laptop by family and other non-work-related employees.

3.5 Change of Use

- The encryption software that is applied to the Companies' laptops will not allow an unauthorised user to log onto a laptop, even if they have a user account from the Companies.
- Where there is a change of allocated user of a laptop due to a leaver or other employee's changes, the line manager must ensure the laptop and any other personal issue equipment is recovered and is then returned to the IT Department for reconfiguration prior to being re-issued.

3.6 Disposal of Laptop

Laptops that are no longer required due to any reason must be returned to the IT department for secure disposal. IT will ensure that:

- Laptops, as any other information security related asset, are removed or updated on the Companies' asset register to indicate that the equipment is no longer in the Companies' control.
- Prior to disposal, all confidential information stored on laptops is backed up using secure technology suitable to the restriction level of the data held
- They receive the necessary confirmation that the storage media within the laptop has been erased or destroyed to a sufficient level and has been disposed of securely.

3.7 Mobile Devices and Services

Company issued mobile devices and services remain property of M Group Services companies' and the Mobile Device Usage Policy - MGS-POL-IT-007 provides further guidance on the use and management of company issued mobile devices and services.

3.8 Company devices

Employees are prohibited from accessing or using streaming services such as Netflix, Hulu, Amazon Prime Video, Disney+, YouTube, or any other similar platform such as Spotify on company-owned electronic devices. This includes, but is not limited to desktop computers, laptops, tablets and smartphones provided by the Company.

The Company implements network-level restrictions to block access to known streaming service websites and plications. This measure is to ensure the Company's compliance with copyright laws and to maintain optimal network performance for business-related activities.

The IT department will regularly monitor network traffic and usage patterns to identify any attempts to access streaming services. Any violations of this policy may be subject to disciplinary action.

3.9 TVs

Televisions provided by the company must be used exclusively for business purposes. This includes training, company presentations, displaying rolling news broadcasts of BBC news and Sky News and other approved uses. Any other use must be expressly authorised.

Employees are prohibited from using company televisions to display or stream copyrighted content that is not licensed for public performance. This includes movies, TV shows sports event

and other entertainment content. Unauthorised use of televisions within the workplace may result in disciplinary action.

4. Removable Media

Removable or portable media storage traditionally includes, but is not limited to the following technologies:

- Universal Serial Bus (USB) memory sticks
- MP3 music players
  Removable hard drives
- Read/write CDs or DVDs • Magnetic tapes and cassettes.
- Memory cards
- Bluetooth capable devices
- Mobile phones

This section is not specific to any of the above technologies but is designed to apply to any current and future removable storage devices. It directs that security controls and countermeasures must be established rather than dictating how to establish them.

All personnel and third parties who have been authorised to use removable storage media must comply with the company controls in place.

4.1 Risk assessment and Authorisation

The necessity for the use of removable storage media must be risk assessed and the use of removable storage media must be authorised by the IT Department.

Only approved types of removable media may be used. The IT Department can advise on which devices are approved for use as these may change from time to time. Approved removable media may only be purchased via the IT Service Desk who will ensure that it is properly recorded in accordance with the relevant Asset Management Policy.

4.2 Security Awareness and Responsibilities

The IT Department maintain asset control procedures and can account for all issued removable storage media within the Companies' against recorded owners and business units. Users of removable storage must understand and comply with the following:

- Protectively marked information or Person Identifiable Data (i.e., that which is subject to the Data Protection Act 2018 & GDPR) must not be held permanently on removable storage media.
- The removable storage media should be used as a mechanism to transfer information and data to more secure, permanent media storage solutions.
- Employees issued with removable storage media are responsible for the security of the device and the information contained within the device.
- Removable storage media must be kept in a secure environment at all times.
- Third parties' agreements must state security controls regarding the acceptable use of removable storage media containing the Companies' information.

- Only Company issued and authorised removable storage media will be used by employees within the Companies' network.

4.3 Technical Security

Removable storage media that contains protectively marked information or Person Identifiable Data (i.e., that which is subject to the Data Protection Act 2018 & GDPR) must be encrypted and have password protection. The Information Security Manager will advise on approved media that may be used for this purpose.

Removable storage media that has been used in an external or private network cannot be used within the Companies' network unless it has been subject to anti-virus scanning. Where it is necessary to store data on removable media longer than the media lifetime (in accordance with manufacturers' specifications), an appropriate secure secondary back-up of the data must exist to avoid information loss due to media deterioration. The IT Department will be able to advise on any actions to be taken.

Removable storage should be encrypted.

4.4 Disposal of Removable Storage Media

Issued removable storage media that is no longer required must be returned to the IT Department.

If removable storage media is to be reused, then the contents of the media must be deleted or destroyed to an acceptable level of non-recovery. This should be arranged with the IT Service Desk via a service request.

If removable storage media is not to be reused, then the device must be returned to the IT Department, who will ensure it is destroyed to an acceptable level of non-recovery. When removable storage media is destroyed, data destruction certificates must be provided to evidence that the Companies' data has been destroyed to a level consummate with the protective marking of the data.

The IT Department must ensure that disposal and destruction of removable storage media complies with the relevant data retention policies and legislation (e.g., Data Protection legislation, WEEE etc.).

5. Internet Use

M Group companies will provide an employee with access to the Internet if this is necessary or helpful to the performance of their work. Where an employee has been provided internet access, they may use the internet at work on the understanding that such access is provided primarily for business purposes.

Not all employees need access to the internet at work. If an employee does not have access but believe they require it, they should contact their line manager.

5.1 Sensible Internet Use

Where employees are granted access to the internet at work, they are expected to use it sensibly, appropriately, and in such a manner that it does not interfere with the completion of their work. If this trust is abused, the Company reserves the right to alter the policy in this respect. Employees should not spend excessive time during work hours (i.e., in excess of their specified break times) browsing the Internet for non-business purposes.

`Guest' Wi-Fi for use with BYOD (Bring your own device) may be available, staff are welcome to use the guest Wi-Fi network for use on personal devices during break and lunchtime. Guests must not knowingly connect devices infected with viruses, malware, or spyware. Please be aware that the same rules within this policy apply to the use of personal devices when on the Companies `Guest' Wi-Fi.

5.2 Personal Internet Use

Internet access is provided for business use; however, it is understandable that employees may, on occasion, need to use the internet for personal purposes and authorises this use provided that:

Use is limited to break times unless permission is granted by a manager

- The internet is not used to access offensive or illegal material, for instance material containing racist terminology or nudity
- Contracts or commitments are not entered in under name of or on behalf of the Company
- Goods are not ordered on the Internet to be delivered to the Company address or order them in the Company's name.

5.3 Registering on Websites

Many sites that could be useful require registration. Employees wishing to register as a user of a website for work purposes are encouraged to do so however, they should seek permission from their line manager before doing so.

5.4 Licences and Contracts

Some websites require the Company to enter into a license or contract terms. The terms should be printed off and sent for approval in advance or emailed to the IT department before an employee agrees to them on the Companies' behalf. Employees should, however, consider whether the information is from a reputable source and if it is likely to be accurate and kept up to date; as such contract terms will exclude liability for accuracy of free information.

It is very important that Sites Privacy agreements are assessed to ensure they meet the requirement of Data Protection law. Do NOT enter ANY agreements with Internet providers that involve personal information.

5.5 Using Other Software and Hardware at Work

The companies comply with all licensing terms and conditions relating to software it purchases. To support in fulfilling its obligations, employees should:

- Only install software on a PC if it is for the business purposes of the Company and approval has been obtained from the IT department. All software installed on a PC or Laptop is automatically recorded in the companies' auditing systems.
- Never load software onto a PC without prior approval from the IT Department. Random audit checks are performed, and any identified infringement of this policy could potentially result in disciplinary action.
- Never copy or distribute software developed or used by the Company unless specifically authorised to do so
- Any employee found to be abusing their internet usage may be subject to disciplinary action which could ultimately lead to their dismissal.

5.6 Using the Internet Safely

ALWAYS:

- Identify yourself honestly and accurately if required to do so;

- Be guarded about the nature of any business or personal information which you transmit via the Internet;
- Report to management any abuse of the Companies' Internet facilities of which you become aware;
- Use downloaded software in accordance with its license;

NEVER (this is not an exhaustive list):

- Use the Internet to engage in any illegal activity (this includes file sharing and downloading copyright materials such as films, books, games);
- Take any action which gives rise to any liability on the part of the Company or its employees unless you have express authority to do so;
- Disclose your password to any other person (if you have been provided with a password to enable you to have Internet access);
- Deliberately introduce viruses or take any other action when using Internet to disrupt, disable, damage or overload any computer system or network, or to circumvent or defeat any system intended to protect the privacy or security of the Company or any third party;
- Download:
    - Entertainment software or games from the Internet or play games against opponents over the Internet;
    - Software from the internet unless you have received authorisation from both your line manager and the IT department;
- Upload or transmit over the Internet any software licensed to the Company or data owned or licensed to the Company without explicit authorisation from the manager responsible for the software or data concerned.
- Participate in online gambling (for personal use or gain or otherwise)
- View, download, print or store any pornographic material or material of a paedophilic or sexually explicit nature or material that would be regarded as illegal or offensive on the grounds of sex, race, age, or disability.
- Use the Company network and/or online services for personal gain, or for personal/private advertising. This includes promoting or campaigning for political, personal, or religious causes.
- Use another staff member's username or password to access an online business account.

5.7 Removing Internet Access

Employees may be asked to justify the amount of time they have spent on the internet or the sites that they have visited. The Company reserves the right to deny internet access to any employee at work if internet use is deemed to be excessive or inappropriate.

6. E-mail Use

Employees are provided with the relevant Company email addresses where appropriate for their job. All employees must ensure that their use of email is compliant with policies and procedures relating to the handling and transmission of classified data.

Where necessary, we may request access to open and read your emails during absence from work e.g. due to sickness or holiday, or when your employment has ceased. This must be approved by an appropriate level of management.

6.1 Content of Emails

Emails that employees intend to send should be checked carefully. The standards expected in relation to the content of email communications are the same as those expected in any other methods of business communication; what is normally regarded as unacceptable in a letter or in conversation is equally unacceptable in an email communication.
Users should be aware that email correspondence is admissible as evidence in legal (or disciplinary) proceeding

The use of email to send or forward messages which are defamatory, obscene, or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure. In serious cases this could be regarded as gross misconduct and lead to dismissal.

If an employee receives an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, they should not forward it to any others. An example of statements to avoid in emails include those criticising the Company's competitors or their staff, those stating that there are quality problems with goods or services of suppliers or customers and those stating that anyone is incompetent.

6.2 Personal Use of Emails

Although the email system is primarily for business use, it is agreeable that the occasional personal use during break times can be done. Personal use should not interfere with your productivity or that of others or disrupt normal business activity. When sending personal emails, employees should show the same care as when sending work-related emails and mark email as ‘Personal’.

If there is evidence that this facility is being abused, we reserve the right to withdraw the use of email for personal correspondence.

6.3 Forwarding and Attachments

Employees should exercise care not to copy emails automatically to all those copied into the original message to which they are replying. Doing so may result in disclosure of confidential information to the wrong person.

Employees should not attach any files that may contain a virus to emails, as the Company could be liable to the recipient for loss suffered. M Group Services have virus-checking in place but, if in doubt, employees should check with the relevant IT department. Employees should exercise extreme care when receiving emails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

6.4 Email Signature

Employees should ensure that all emails, including replies, have the official corporate information detailed on them which should contain the relevant contact information of the individual as per email signature guidelines available on M Connect.

6.5 Using Email Appropriately

Employees are provided with email facilities to enable a rapid and efficient method of internal and external communication for business purposes. All employees who are provided with these facilities are expected to:

ALWAYS:

- Identify yourself honestly and accurately;
- Mark all sensitive e-mail messages accordingly;
- Protect all email messages stored on your computer by means of a password. (The password should be kept confidential and should not be disclosed to any person unless this is specifically authorised by an appropriate manager);
- Mark all personal email as “personal” in the subject field of the message;
- Ensure that the transmission of personal email does not give rise to any liability on the part of the Company or its employees;
- Report any abuse of e-mail facilities of which you may become aware.

NEVER (this is not an exhaustive list):

- Send e-mails which are abusive or defamatory or contain bad language;
- Send, distribute, store, or print e-mail of a sexually explicit, racist, or offensive nature, or invite or encourage others to do so. We recognise that it is not always possible to control

incoming e-mail, but should you receive any material of the kind described above, you should report it immediately.

- Agree to any terms or enter into any contractual commitment on behalf of the Company unless you have the proper authority to do so;
- Open email attachments which are received from a suspect source. If in doubt, you should seek advice from the IT Department
- Waste time or cause disruption by distributing non-business e-mails to colleagues at work;
- Send chain letters, or advertising material which does not relate to the Company's business;
- Use the Companies' email facilities for the purposes of any business other than the Companies' business;
- Use email to distribute videos, graphics files, sound files, software, or other complex attachments unless this is for the business of the company, and you have been expressly authorised to do so by an appropriate manager;
- Attempt to gain access to email messages addressed to any other employee without first obtaining authority from the addressee or an appropriate level of management;
- Use email to communicate sensitive personal details about yourself or others
- Use email to send corporate or customer information to personal email accounts to enable remote working or for other purposes.

7. Other communication applications

There are approved applications for communications across the business such as Teams, StayConnected etc. We expect that all employees will conduct themselves in a professional manner when interacting with others or when managing colleagues whilst using the communication tools available. These communication tools should not be used for unacceptable communication behaviours such as bullying, harassment, aggressive and coercive or intimidating behaviour amongst others. This will be thoroughly investigated by the HR department with support from IT.

8. Social Networking

The Internet provides many ways in which to communicate, including sites such as Facebook, blog sites and other third-party sites.

Due to the nature of the contracts and processes within some business units, you will be restricted from communicating with the majority of these sites including Internet chat rooms, news groups, social network sites or similar sites, unless you have been expressly authorised to do so for a legitimate business purpose. Communication with such sites for private purposes using Company facilities is NOT PERMITTED at any time, including whilst working at home.

8.1 Referencing the Company on Social Networking Sites

Where sites or groups show any association with, or make reference to the Company, employees are expected to behave appropriately and in ways that are consistent with M Group Companies' values and policies, even when using their own personal computers. This includes, for example, sharing photographs or videos showing employees in company uniform, on Company premises or in Company vehicles.

Employees should not post photographs, videos, or other such material of their work colleagues, without their express permission, even where the photos have been taken outside of the working environment. They should also remove information about a colleague if that colleague asks them to do so.

We recognise that external parties may utilise such sites to create negative publicity about the M Group Services Companies. Employees who come across such sites are reminded of their responsibilities under this policy and requested to report such sites to their manager or the IT department.

Employees may find themselves subject to prosecution by the Company or individuals if they breach this policy.

Employees should not express opinions over the Internet that purport to represent the views of the Company.

8.2 Using Social Networking Sites Responsibly

The guidelines below must be adhered to when using the Internet for personal use on your own computer:

ALWAYS:

- Be mindful of the information disclosed - through the open nature of the Internet, it is easy for third parties to collate vast amounts of information and it's not always easy to be sure of the identities of people who visit sites or view information.
- Behave the same way online as you would offline - don't post anything that someone wouldn't want to be overheard saying or seen doing.
- Check the privacy settings of the Social Networking site and limit access to known and trusted people - although most sites do have privacy options, few, if any, guarantee 100% security.
- Remember that most items that are posted on Social Networking sites are permanent even after removal, copies may remain viewable in cached and archived pages, or if users have copied or stored the contents - even if what has been written has been written privately, it is possible that someone else may quote it publicly.

- Think about personal safety and do not create unnecessary risks by disclosing contact details.
- Remember you are at risk of being documented on social media by members of the public if you are acting inappropriately whilst you are representing the Company

NEVER (this is not an exhaustive list):

- Use the Internet to attack or abuse colleagues - offensive comments about colleagues may amount to cyber-bullying and could be viewed as a disciplinary matter.
- Disrespect the privacy and the feelings of others - posting derogatory or offensive comments or something defamatory could result in action being taken
- Act in a way which might bring M Group Services into disrepute - if an employee's conduct on Social Media causes offence, this may be treated as misconduct and in serious cases this could be regarded as gross misconduct and lead to dismissal.
- Accept payment to produce or contribute to a blog for a third party without discussing this with your line manager before - this could constitute a conflict of interest (blogs or websites which do not identify the blogger as an employee or reference the Company and are purely about personal matters would normally fall outside this guidance).
- Use the Internet to download applications or stream media which utilises bandwidth unnecessarily and as a result slow down business usage.

9. Remote Users

Employees will sometimes need to use the Companies' assets or facilities and to access the Companies' network when working remotely, whether from their home, a non-Company site or when travelling.
Remote users are reminded that this policy applies to them wherever they are using the Companies' assets, facilities and when accessing the companies' network. Remote Users shall also comply with the requirements of this policy.

Only Company approved Remote Access solutions are to be used, and use of unauthorised 3rd Party remote access solutions, such as logmein.com & GoToMyPC, are strictly prohibited. Please refer to the HR Agile Working Policy for more details on remote working.

10. Home Working

There may be circumstances where individuals will either need to or be required to work based at home rather than at their normal place of work and may thus involve using Company IT systems to conduct their duties whilst they remain in contact with managers and colleagues. This may be carried out to an agreed work pattern on either a permanent, regular, part-time, temporary or on an ad hoc basis.

Whilst not all job roles are suitable for home working, reasonable effort has been put in place by the Companies' IT systems to ensure the systems are robust enough to support working from home. Managers however must ensure that home working arrangements are made with appropriate security measures for IT systems prior to approving working from home.

10.1 Information Security

All colleagues working from home must ensure that they adhere to the Companies' Information Security and Data Protection policies, procedures, and guidance. Any other relevant policy, procedure and guidance must also be adhered to.

The Companies' IT department will ensure that all home workers have a process for secure remote access to the IT systems as required. The usual monitoring of the use of internet, email and general IT systems access will be carried out.

Whilst working from home, the requirements of this Acceptable Use Policy still apply. The individual should further:

- Confirm the necessary equipment provided is in good working order and is suitable to conduct the necessary requirements of their role
- Abide by the working from home health and safety requirements in the use of company equipment in line with risk assessments conducted.

10.2 Staff Security Guidelines

All staff must ensure that they manage their own security at home. The items below will vary depending personal circumstances; however, staff must contact their line manager if they feel their working environment is not secure enough for their role.

- Consider the working area you intend to use. Ensure that, wherever possible, you can close the door and that your screen(s) are not overlooked by others and your conversations are private.
- Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.
- Do not leave confidential material on desks, workspaces, or other parts of the house.
- Please save confidential written material for office visits to be securely destroyed. If necessary, or possible, use a paper shredder for your home environment.
- Follow all company Information Security policies as if you are in the office.
- Ensure that data is backed up to the network.
- Connect to the network via a VPN. All company machines should have this installed.
- Do not use your own personal equipment to store company data.
- No family members may use any company provided equipment.

- Read Company IT notices as these will contain advice on threats and changes to the system.
- If you have any security doubts, contact your IT Service Desk.
- Complete the fundamental IT Security and data Protection course if required.

11. Lost or Stolen Assets

Portable IT equipment, such as laptops, tablets or HHT, smartphones and removable storage media are particularly vulnerable to theft or loss and adequate security measures should therefore be taken to safeguard the confidentiality, integrity, and availability of these assets.

Lost or stolen information technology assets (e.g., laptops, smartphones, tablets, removable storage media etc.) must be reported immediately as an Information Security Incident – if in any doubt, seek guidance from the appropriate line manager. Lost or stolen assets should also be reported to the police and a crime reference number obtained (see guidance in section 2.5).

Any loss of assets, where the risks have not been adequately mitigated in line with the guidance in this policy could result in disciplinary action and/or employees being required to pay the cost of replacing the equipment.

12. Monitoring

In order to safeguard the Companies' systems from the risks referred to in this policy and to maintain the confidentiality, integrity and availability of the network and the accountability of individuals, we have the right to monitor all of the IT assets and facilities that are made available to users and to monitor, intercept and/or record any communications made by employees, including e-mail, local-area-network, or internet communications.

Any monitoring will be carried out subject to the requirements of legislation including the Data Protection Act 2018 and GDPR, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, and the Telecommunications Regulations 2000. Monitoring may be carried out for any purpose authorised by legislation.

Employees are required to co-operate and assist, as necessary, with any monitoring carried out in accordance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

It is the Companies' intention that any monitoring will be proportionate, taking into account the risk(s) of harm to the interests of the company, and the extent of any intrusion into the privacy of users.

12.1 Internet Monitoring

The monitoring of internet usage is conducted for reasons of security and efficiency and to ensure compliance with the law and with the provisions of this policy. This may take the form of random monitoring or spot checks, audits, interception or filtering of communications and collection of traffic and usage data and covers both incoming and outgoing email as well as Internet usage. Monitoring methods may be manual, automated or both.

Responsibility for monitoring may be outsourced and may take place for any of the following purposes:

- To establish the existence of facts relating to the Company's business (e.g., the contents of communications with customers relating to contractual matters).
- To ensure that all relevant laws and regulations are being complied with.
- Where there is a requirement to satisfy a Data Protection Act Subject Access Request.
- To prevent or detect crime.
- To prevent or detect the unauthorised disclosure of the Company's confidential information, or the use of unlicensed software.
- To ensure that there is no abuse by employees of privileges relating to personal use of e-mail and Internet facilities.
- To detect the transmission of inappropriate material.
- To enable business matters to be dealt with during an employee's absence from work.
- To protect the Company's systems from viruses or overloading and to safeguard and monitor the security and integrity of those systems.
- To ensure that the provisions of Group and individual company and departmental internet policies and the Computer User's Good Practice Guide are being complied with.
- To ensure that other Company policies and requirements are being complied with (for example relating to equal opportunities, sensitive information, and employment restrictions).
- If the Company suspects that the employee has been spending an excessive amount of time viewing websites which are not work related.
- The Company reserves the right to retain information that it has gathered on employees' use of the internet for a period of one year.
- Ongoing validation of compliance with Internet & Email policy.

All monitoring will be proportionate to the relevant objective and information obtained will only be used for the legitimate purposes of the Companies' business.

12.2 Email Monitoring

The companies' reserve the right to monitor employees' emails. The circumstances under which such monitoring can be undertaken requires the approval of the IT Director and the Director of the individual concerned.

The following is considered to be examples of valid reasons for monitoring an employee's email (NB this list is not exhaustive):

- If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue
- If the company suspects that the employee has been viewing or sending offensive, inappropriate or illegal material, such as material containing racist terminology or nudity (although we understand that it is possible for employees to inadvertently receive such material and they will have the opportunity to explain if this is the case).
- If the company suspects that an employee has been using the email system to send and receive an excessive number of personal communications.

- If the company suspects that the employee is sending or receiving emails that are detrimental to the M Group Services Companies.

In view of the possibility that e-mail communications will be monitored for the purposes set out above, employees should not use email to communicate sensitive personal details about themselves or others.

When monitoring emails, we will, save in exceptional circumstances; confine itself to looking at the address and heading of the emails. Employees should mark any personal emails as such and encourage those who send them to do the same.

We reserve the right to retain information that has been gathered on employees' use of email for a period of one year.

12.3 Monitoring and Charges

Usage of data, calls and texts will be monitored as excessive personal use is prohibited. Data usage for the downloading of applications, internet services and media streaming on any communication device should be limited to business and work use only. Abuse of data as itemised on the monthly bills may be subject to repayment and/or disciplinary action.

International calls, premium rate calls, excessive texts, or premium rate texts, calls to gambling lines or book makers, excessive volumes of personal calls or any calls that could potentially bring the Company into disrepute are not permitted.

The Company reserves the right to request payment where personal use, as itemised on a monthly bill is considered excessive.