# IT POLICY

**Policy Statement: Information security policies are the principles that direct managerial decision making and facilitate secure business operations. They allow the organisation to manage the security of information assets and maintain accountability. This Policy covers protocols and procedures for use of the company's IT equipment, specifically its servers, networks, and broadband connections. It also includes devices issued by the company including laptops, tablets, phones etc. as well as any equipment owned by staff or third parties which the company permits to be connected to its network. This policy should be read in conjunction with the Acceptable IT Use Policy and Data Protection Policy. This policy gives the organisation a structured framework to properly manage IT resources.**

**All Employees:** This policy applies to all persons working for or on our behalf of the McSence Group of Companies which includes the subsidiary companies - *McSence Communication Ltd, McSence Ltd, McSence Services Ltd & McSence Workspace Ltd* in any capacity including but not limited to:

- Directors, all employees at all levels, prospective employees, agency workers, seconded workers, temporary workers, contractors/sub-contractors, clients, agents, external consultants, volunteers, members of the public, group's supply chain, third-party representatives and/or business partners who will be referred to in our Group policies as "all employees".

**The Workplace:** This policy applies to all persons working for or on our behalf of the McSence Group of Companies in any capacity at the workplace(s) as defined below which includes but not limited to:

- McSence Premises, Offices, Units, Business Park, Client's Premises, External Meeting Places, Customers' Homes, Gardens, Sheltered Housing, Whilst On-Call, On-Duty, Emergency Cover, Working from Home including On-Line Meetings, Whilst Driving in Company Time, Working Public Areas (café's, trains, coffee shops, buses etc) and will be referred to throughout this policy as "the workplace".

**Purpose:** McSence must ensure our IT systems operate efficiently, securely, and safely to protect our data and that of our clients, comply with GDPR and remain protected from cyber attacks or other digital threats. It is also important to ensure consistency of approach in the use of our IT systems. Employees have an obligation as far as reasonably practical to assist in this objective.

**Roles & Responsibilities: Employees:** Employees are required to follow the procedures set down in this Policy and to operate in a way which protects the best interests of the Company. In particular:

- Employees must be aware of cyber security issues and keep the company's equipment and data safe as far as reasonably practical.
- Employees must keep all passwords secure and personal to them and not share these with colleagues or anyone outside the business. Passwords should not be written down and should especially not be left where others might find them.
- Employees must ensure passwords selected are secure by following the guidance later in this document. Passwords must be changed regularly in accordance with this Policy.
- Employees must ensure the security of all company issued equipment and report anything lost or stolen immediately they become aware.
- Employees must report any breaches or incidents likely to lead to a breach in this policy or any other general cyber security issues to their Business Unit Manager or the Chief Executive as soon as they become aware.
- Failure by an employee to follow the IT Policy as set out within this document will be considered a conduct issue and may be subject to action under the company's disciplinary procedure.
- A deliberate act of sabotage in the use of any Company IT systems or equipment or deliberately passing access information such as passwords to other parties with the intent of causing harm to the Company or its stakeholders will be regarded as gross misconduct and will be subject to action under the company's disciplinary procedure.

**Business Unit Manager:** The Business Unit Manager is responsible for supervising their staff in complying with the requirements of this Policy. In particular:

- The Business Unit Manager will advise the Chief Executive of all new staff starts, the equipment they require to carry out their role and what if any access is required to the Company's IT systems.
- The Business Unit Manager will monitor all employees under their control who are accessing Company IT systems and ensure adherence to this Policy.
- The Business Unit Manager will monitor all company IT equipment and resources issued to staff under their control and report any repair or replacement requirements to the Chief Executive. Managers should be aware at all times of where equipment allocated to their departments is and must report any missing or stolen equipment as soon as they become aware. A regular audit of where equipment is, should be carried out.
- The Business Unit Manager will advise the Chief Executive in a timely manner of all staff who need to have access permissions altered, restricted, or terminated by reason of leaving employment, changing role, long term absence, suspension, or disciplinary actions or for any other reason where their continued access to data or equipment could compromise the business.
- The Business Unit Manager will assess the IT competence of all new staff joining or being promoted or transferred into a new role maintain and maintain a record of this in their Training Matrix. This should identify any training needs for which the Business Unit Manager will be responsible for implementing.
- The Business Unit Manager will keep the Chief Executive informed of any recommendations for change or updating required to this Policy to support the Company's objectives.

**Chief Executive:** The Chief Executive has ultimate responsibility for this Policy and will act as the lead officer for all IT related issues. In particular:

- The Chief Executive will keep this policy under review and will update, as necessary.
- The Chief Executive will be responsible for appointing an experienced and competent IT Support Contractor and will review their performance from time to time.
- The Chief Executive will be responsible for maintaining suitable Cyber Protection Insurance assuming such insurance remains available in the marketplace at competitive rates.
- The Chief Executive will be responsible for specifying, sourcing, and procuring suitable IT equipment and devices and will maintain an Asset Register of all such equipment owned and operated by the Company.
- The Chief Executive, through the IT Support Contractor, will arrange access to IT systems and levels of access and authority including the issue of passwords as advised as being required by the Business Unit Managers.
- The Chief Executive may delegate some or all his responsibilities under this policy. All such delegations should be recorded in writing unless temporary due to absence in which case his duties will be undertaken by his nominated deputy.

**IT Procedures:**

**Support:** The company will procure and maintain a suitable IT support contract to provide remote support for servers, network end user PC's and other IT related equipment. This will essentially be a reactive service to deal with faults and outage issues rather than training needs which should be dealt with separately through normal line management routes. This contract is separate to support for services such as phones and broadband. Current providers are set out below:

| | | | |
|---|---|---|---|
| IT Support: | Network ROI Ltd | 0131 510 1234 | Helpdesk@networkroi.co.uk |
| Phones: | 2 Circle Ltd | 03456 200 200 | |
| Broadband: | 2 Circle Ltd | 03456 200 200 | |
| Security Incident: | CFC Underwriting Ltd | 0800 975 3034 | Policy No: ESJ0224812694 |

**Descriptions of Systems Available:** The Company's IT systems consist of a network accessible by CAT5e hard wired cabling and WIFI access points within the office premises or remotely via a secure Fortinet VPN. The network comprises two servers, one at each office location which are connected together to back each other up and provide redundancy in the event of a hardware failure. A separate off-site cloud backup is also used. Staff can access the network through the McSence domain for which they will receive a username and password. Once connected to the domain, staff can access the internet through our broadband supply or can store and receive data files from our data file servers. Users can only access areas of the data server for which they have been given permission. Company issued machines connect to the WIFI system via the "Staff" network. Staff may also connect their own devices while in the office but only

through the "Guest" WIFI network which gives internet access only. WIFI access passwords are changed regularly and can be obtained from Business Unit Managers.

**Software:** The Company uses a subscription service to Microsoft 365 to provide general Office products such as Word, Excel, PowerPoint etc. as well as an email address for each staff member. Passwords for this are synchronised with the domain logon username and password except for those who do not have domain access. We also use specialist software, largely cloud based applications, such as SAGE for accounting, Staffplan for Care workflow management and Footprint for Property Maintenance and Cleaning Workflow Management. We also use Paxton to control security and access doors at both properties and Fortinet for fire walls, end point virus protection and VPN access. For support with specific software applications, staff should speak in the first instance to their Business Unit Manager who will advise the most relevant source of help. Otherwise, support can be sought from:

| | | |
|---|---|---|
| SAGE (Internal) | Shabana Latif | shabana.latif@mcsence.co.uk |
| SAGE (External) | 0191 479 5955 | McSence Services Ltd Account No:35478800 |
| Staffplan (Internal) | Lee Notman | lee.notman@mcsence.co.uk |
| Staffplan (External) | 01233 722700 | McSence Communication Ltd Account No:008002 |
| Footprint (internal) | Martha Convie | martha.convie@mcsence.co.uk |
| Footprint External) | Ben McGowan | ben.magowan@footprintwfm.com |
| Paxton | John O'Neil | sales@secuirty-control.co.uk |
| Fortinet | Malcolm McGilvray | malcolm@softworx.co |

**New Staff Joining:** Business Unit Managers will advise the Chief Executive of all new staff joining who require access to the Company's IT network, the minimum level of access they need, and what devices are required to be issued. This should be done with as much notice as possible to allow the necessary devices to be procured and set up. New staff joining will generally fall into three categories:

1. Staff who will need a laptop or desktop and will require access to the Company network and data storage.
2. Staff who will not require to use a PC or access the network but who will need a McSence email address to be used on a Company issued device or their own device.
3. Staff with no IT access requirements.

**For staff who fall into Category 1**, the Chief Executive will issue the required devices and arrange for the IT Support Contractor to issue a username and password for access to the network. The username will have restricted access as defined by the appropriate "user group" allocated by the Chief Executive. All company issued devices must be password protected, including mobile phones.

The users first logon to the system will be undertaken during the induction process so that it is supervised by a suitably qualified member of existing staff. The password issued must be changed at first logon by the new staff member in accordance with the password guidance set out below. This can be done as follows:

- Hit "Ctrl" "Alt" "Delete" all at the same time.
- Click on "Change a password"
- Follow the instructions listed on the screen.

Passwords should be changed regularly and at least every two months. If an employee believes their account may have been compromised, they should change their password immediately and advise their Business Unit Manager or the Chief Executive directly.

The Chief Executive will also arrange for the IT Support Contractor to open a Microsoft 365 account to assign an email address to new staff members and give them access to Microsoft Office. Office programmes such as Word, Excel, PowerPoint etc. will be set up on the device and should open automatically as the same password as used to access the network will open Microsoft 365.

**For staff who fall into Category 2**, the Chief Executive will issue the required devices and arrange for the IT Support Contractor to issue a username and password for access to Microsoft 365 to assign an email address to new staff members and give them access to Microsoft Office. These staff will not have access to the network or any server data storage.

The users first logon to the system will be undertaken during the induction process so that it is supervised by a suitably qualified member of existing staff. This will be done by accessing Microsoft 365 over the internet using a Company PC or the users own device. This can be done as follows:

- Navigate to www.office.com
- Click on "sign in"
- Enter assigned email address and click "Next"
- Enter password and click "Sign In"
- You will then be prompted to have a code sent to your mobile phone, select yes
- When the code arrives by text message enter it in the appropriate box and complete sign in
- Click "No" for stay signed in.

On a first sign in users should be prompted to change their password but if not, and for subsequent password changes proceed as follows:

- Click on the settings gear wheel at the top left of the screen
- Click on "change password" on the right-hand side of the settings screen
- Follow the instructions given.

The password issued must be changed at first logon by the new staff member in accordance with the password guidance set out below.

**For staff who fall into Category 3**, no actions are required as these staff do not have access to the Company network or a Company email address.

Users may access Microsoft 365 from their own devices to synchronise their email accounts on their phone for example, but two factor authentication will be required to do so. Staff wishing to do this should seek authorisation from their Business Unit Manager and provide a mobile phone number for the second authentication. When set up by the IT Support Contractor, staff will be able to access Microsoft 365 as outlined above for Category 2 staff.

**Password Guidance:** This section gives guidance on staff as to how to select and use secure passwords.

- **Passwords should be changed regularly, at least every two months**. You may have been hacked and not know. Always make sure you change a manufacturers default password on any device.
- **Never use the same password for different applications**. If one password gets hacked, then they will have access to everything.
- **Never use the same passwords for home and work applications**. A breach of one could allow both to be attacked.
- **Don't write passwords down**. If you struggle to remember them, use a password reminder app such as Dashlane, Lastpass, Myki, LogMeOnce, Keepass, Nordpass, Roboform, iPassword etc. Remember, if you have to pay for an app, it is almost inevitable it will be better and safer than one you get for free!!
- **Don't store passwords in a file on your computer or phone**. That can be hacked too.
- **When you are issued with a password, always change it when you first log in**. Otherwise the person who gave you the password will have access.
- **Do not share passwords with your colleagues or anyone else for that matter**. If more than one user has access to an account, they can be misusing the system and you could get the blame!
- **Do not reveal your password to someone presenting as "IT support" who you don't know**. You might well be being scammed by someone who knows who our IT support are.
- **Do not put passwords in an email or text**. If a hacker has access to our mail system, they also have access to any stored or even deleted messages.

- **Always report a suspected hack**. Once a hacker is in, changing your password may not be enough to keep them out or prevent harm.

**Selecting a password:** Password hacking software is becoming increasingly sophisticated and looks for the type of things we all use to make passwords easy to remember such as children and pet's names, cars, lyrics from songs, film titles, TV programmes or celebrities names. Information you have on social media is often used to crack passwords such as dates of birth, place of residence or birth, partners names, sports teams supported etc. They also look for commonly issued first passwords which users haven't changed such as "password" or "welcome". Make sure you avoid these at all costs. Short passwords are also easier to crack and should be avoided.

To select a strong password:

- **Use a minimum of three random words**. i.e. wondertraintogether
- **More words are better than extra complexity**. Security experts say five words is almost uncrackable.
- **Mix in capitals for extra complexity** i.e. WonderTrainTogether
- **Introduce numbers to replace letters for extra complexity** i.e. W0nderTra1nT0gether
- Mix in special characters to replace letters for extra complexity i.e. W0nderTr@1nT0gether

This can make passwords easier to remember but still incredibly secure.

**WIFI Access on the premises:** There are two WIFI networks available on the premises, one for McSence issued devices which gives full access to the network and one for non-McSence devices which gives access to internet only.

**McSence Devices:** Where possible, McSence devices should be connected to the network by hard wiring as this is more secure and works faster than the WIFI. If connecting by WIFI, the procedure is as follows:

- Click on the WIFI icon on the bottom right of the screen.
- Select **"McSence Staff"** from the list of available networks.
- Tick "connect at logon" box and then click connect.
- Input password when prompted. (The current password can be obtained from the Business Unit Manager)

**Non-McSence Devices:** Staff or visitors may connect their own devices to the guest network in order to obtain internet access but must not connect to the staff network which gives access to the data server and would present a significant security risk. The procedure is as follows:

- Click on the WIFI icon on the bottom right of the screen.
- Select **"McSence Guest"** from the list of available networks.
- Tick "connect at logon" box and then click connect.
- Input password when prompted. (The current password can be obtained from the Business Unit Manager)

**Remote access using VPN:** Staff with company issued devices working from home, in client's premises or other remote locations with internet access, can connect to the McSence network and access data files by logging into the FortiClient VPN app. This is loaded onto laptops when they are being set up and all staff should have this on their desktop. If not, please contact IT Support to have it added. The process for connecting is:

- Click on the FortiClient shortcut on the desktop home screen.
- Click on "Remote Access" on the menu on the left-hand side.
- Enter username (same as domain logon i.e. <first name>.<last name>)
- Enter password (same as domain logon to start laptop.)

The app will then connect, and users can access files from the data drive in the usual way using Windows File Explorer.

Other cloud base applications such as Windows 365, Staffplan, Sage and Footprint can be accessed remotely from any device with internet access using the appropriate username and password. In the case of Office 365, two factor authentication will be required when not using a McSence device.

When connecting to the VPN in this manner, staff must take all possible measures to ensure the internet connection used is secure. Staff must not use publicly available WIFI such as coffee shops etc. and staff working from home should ensure the firmware on their internet router is up to date and protected by anti-virus software. If in any doubt, use company issued mobile devices running 4G or 5G mobile networks by tethering as outlined below.

**Remote access using Tethering:** If there is a need to connect to the network when there isn't an internet service available, staff with a McSence mobile phone can use the data plan to connect their laptop to the internet by tethering. This can be expensive depending on the mobile package in question so should only be used if absolutely necessary. Staff can use their own mobile devices to do this but once again it is expensive. The procedure for connecting is as follows:

**For IOS Users:**

- Click "Settings"
- Click "personal Hotspots"
- Click "allow others to join"
- Note the Wi-Fi password given.
- On laptop, click on WIFI symbol at bottom right of screen
- Click on the name of your phone as displayed in list.
- Click connect.
- Input password when prompted.

This will connect you to the internet using your phone as a hub and you will be able to access the VPN using the same procedure set out above.

**For Android Users:**

- Click settings
- Select Connections
- Select Mobile Hotspot and Tethering
- Select Mobile Hotspot and select on
- Note the Wi-Fi password given
- On Laptop, click on WIFI symbol at bottom right of screen
- Click on the name of your phone as displayed in list
- Click connect
- Input password when prompted

**Email Usage:** The Company uses Microsoft 365 Outlook for its email system as noted above but for this policy, email is described as any computer-based messaging including notes, memos, letters and data files that may be sent as attachments.

All email on the McSence systems, including personal email, is the property of McSence. As such, all email can and will be periodically monitored for compliance with our policies.

Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members, such as Microsoft Teams. In all other cases, no user is authorised to open or read the e-mail of another without the express consent of their Business Unit Manager.

Staff must not forward Company email information to their own personal email accounts or those of any other user unless there is a clear business need to do so and authority has been granted in advance by their Business Unit Manager.

The Company uses an automated cloud backup service for its 365 system and any lost or misplaced emails can be retrieved by making a request through the IT Support Contractor. As such, staff should note that deleting an email message does not mean it has been deleted from the system.

Staff leaving the business for whatever reason must not take Company information or data of any kind from the email system.

**Data Storage on the Company Server:** Data files are stored on the server in a drive entitled "Data", the address for which is \\mcsence.local\data. This is generally labelled as Z: drive although some users may see it as U: Drive. The drive is organised into a number of folders relating to Business Units or activities with a number of Group folders for commonly used files. This folder structure can only be altered by the Chief Executive or the IT Support Contractor and any requests for charges to this should be made directly to the Chief Executive. All folders are secure and can only be accessed if specific permission is given to that user. The Chief Executive and the IT Support Contractor maintain a list of User Groups to which all new account holders are allocated depending on their level of access. Should a user find they need access to folders that they don't currently have, permission should be sought from the Chief Executive for their User Group allocation to be changed. Similarly, if users discover they have inadvertently been given access to a folder they shouldn't, this should be reported immediately to the Business Unit Manager or directly to the Chief Executive.

The file architecture within each departments folder is a matter for the Business Unit Manager to arrange and order to suit their specific needs. Staff may open a personal folder within this for storing their own personal information in accordance with the Acceptable Computer Use Policy. Any personal information placed on the company's servers becomes the property of McSence.

Staff should not save files to the hard drive of their PC or laptop except in an emergency or as a temporary measure for a very short period of time as this is not backed up and cannot be controlled by the Company's data use or GDPR procedures.

All Company devices are set up with a shortcut to access the Data Drive from the "This PC" screen in Windows File Explorer. The procedure to access this is:

- Open Windows File Explorer
- Click on "This PC" on the menu to the left of the screen
- Click on the icon "data(\\mcsence.local)

If a user is accessing from a machine they have not used before it may be necessary to map the network drive for your profile before you can see this icon. This can be done as follows:

- Open Windows File Explorer
- Click on "this PC" on the menu to the left of the screen
- Click on "Computer" on the very top tab at the top of the screen
- Click on "Map network drive" on the banner at the top of the screen and select "map network drive".
- On the next screen What network folder would you like to map?
    - Select Z in the drive box.
    - Type in the folder box \\mcsence.local\data
    - Tick the "reconnect at sign-in" box
    - Click "finish"

This should then take you to the data folder.

**Data Backup Procedures**: All data on the server is automatically backed up between the two servers at HQ in Mayfield and in Galashiels on a continuing rolling basis and also daily to an off-site cloud service provided by Arcserve. If users accidently lose any data, it can be recovered by making a request through the IT Support Contractor. Staff must not

make their own backup copies of any McSence data as this would be outwith our control and thereby a breach of our GDPR regulations.

**Data Security:** The security of the Company's data is of paramount importance. Any loss of data or breaches in our security protocols could result in a breach of our obligations under the GDPR regulations which could have severe financial consequences for the business. In addition, we handle very sensitive personal information on our Care clients and any loss of mistreatment of this could result in the withdrawal of our Care Inspectorate accreditation which would mean we would not be able to trade.

In order to protect data, there is a limit in the number and size of files that can be downloaded from the server to other devices or placed as attachments within an email. Any staff who have a specific business need to exceed this limit can seek authorisation from the Business Unit Manager.

Similarly, Company devices are set to limit download of data from the server to the hard drive or external peripherals such as USB memory sticks or CD drives. Any staff who have a specific business need to exceed this limit can seek authorisation from the Business Unit Manager. Only Company issued encrypted USB memory sticks can be used in Company issued devices.

Company mobile phones should not be used to store any data, nor should they be used to download any non-company approved apps. Under no circumstances should staff download apps from any source other than an approved apps store and only then with the written consent of the Company.

While we have automated procedures in place to protect data, most breaches are caused by human actions and all staff must play their part in ensuring our data remains secure. Any failure to comply with this policy by a member of staff which results in a data breach may be regarded as gross misconduct and likely to result in disciplinary action.

**Internet and Cyber Security:** Internet use represents the single largest risk to cybersecurity for the Company. The network is protected by a Fortinet firewall which offers protection from hacker attacks and limits the type and nature of websites that staff can access. However, like all technology, it is not infallible, and staff must take care when accessing the internet and only visit secure sites necessary for their duties. Staff should also comply with the Acceptable Computer Use Policy at all times.

All McSence devices are set to install security updates and patches automatically. Staff must not change this setting on their device. If staff become aware devices are not automatically updating, they should bring this to the attention of the IT Support Contractor immediately. Some updates require devices to be re-booted in order to fully install. If staff receive a request to re-boot, they should do so as soon as convenient. This includes company issued mobile phones.

Devices should be shut down when not in use, particularly overnight, and must not be left connected to the network when unattended, particularly when working remotely via the VPN. This is to prevent cyber-attack as devices are more vulnerable when left switched on an unattended for significant periods of time, but it also helps to save electricity.

Some staff may require access to a wider selection of websites as part of their job for example research purposes, in which case they should make an application to the Chief Executive for restrictions to be reduced stating what access they require and for what purpose.

As a final level of defence, the Company maintains comprehensive Insurance cover for cybercrime which includes an incident management service. If a member of staff becomes aware of a potential cyber breach, they should immediately inform the Chief Executive or the IT Support Contractor who will contact the Insurers.

While we have automated procedures in place to protect against cyber-attack, most breaches are caused by human actions and all staff must play their part in ensuring we remain protected by familiarising themselves with basis cyber security measures such as:

- Selecting secure passwords, changing these regularly and not divulging to anyone else.

- Not visiting high risk web sites.
- Not connecting to the internet from unsecure, open or public internet connections.
- Not clicking on any links contained within email from unknown sources.
- Not clicking on any links contained within unsecure websites.
- Not accessing social media from company devices.

Any failure to comply with this policy by a member of staff which results in a cyber security breach may be regarded as gross misconduct and likely to result in disciplinary action.

**Printers and other peripherals:** The Company have a number of networked Xerox copiers which also provide printing and scanning facilities. These are metered to allow the Accounts Department to attribute printing costs across the Group except for the Care offices where the Xerox machines are dedicated to those departments. Each department has a pin code to access the printers which is available from the Business Unit Manager or Accounts department. The use of standalone laser of inkjet printers is discouraged due to the cost but some are available and can be allocated by reference to the Chief Executive.

Company issued devices are pre-loaded with the necessary Xerox drivers and should be visible from the drop-down printer menu. To access this:

- Click on “File” at the top left of the screen.
- Click on “Print” on the menu on the left of the screen.
- Click on the “Printer” drop down menu and select the appropriate printer.

If the printer you want is not shown, you can install the driver as follows:

- Click on the Windows symbol at the bottom left of the screen.
- Click on the settings symbol at the bottom left.
- Click on “Devices”
- Click on “printers and scanners”
- Click on “add a printer”
- Click on “the printer I want isn’t listed”
- Click on “add a printer using TCP/IP address”.
- Click “next”
- At “list name or IP address” type:
    - 192.168.0.219 for the Mayfield main office printer
    - 192.168.0.217 for the Mayfield Care office printer
    - 192.268.0.218 for the Mayfield Training office printer
    - 192.168.12.200 for the Galashiels office printer
- Click “next”
- Click “do not share”
- Click “next”

The driver will then be installed and identified as a number. Once installed you can change this if you want to something more recognisable like Main Office Printer by changing the name of the printer in “Printer Properties”

**Using your own device (BYOD):** The Company recognises that personally owned equipment can play a valuable role in convenience, efficiency and productivity and as such permits staff and others visiting the premises to bring their own device to work but these should not be used to connect to the staff network or to access files stored on the Company network. They should only be connected to the “McSence Staff” WIFI network as noted above. While this will leave them isolated from our main network, there is still a level of risk and Staff must comply with the same cyber security measures as they would if using Company issued devices such as:

- Password protect all personally owned devices and don’t share passwords with others.
- Install a good virus protection software package.

- Do not leave personal devices unattended.

The following is a list of personally owned devices permitted:

- Laptop computers
- Tablets
- Personal digital assistants (PDAs)
- Smart phones
- Portable music players

When using their own personal devices, users must comply with the organisations Acceptable Computer Use Policy and all other Policies and Procedures in place just as they would if the device was owned by McSence including reporting any security issues on their own devices if these have been connected to the McSence network.

The organisation reserves the right to install a digital certificate on each personally owned device which will authenticate the user and reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network.

In the event of a suspected data security incident, McSence may take and confiscate a user's personally owned device at any time. In such an instance, the organisation reserves the right to wipe the user's personally owned device at any time. Not only will company data be wiped, but the user's personal data could be lost as well. The user must understand and accept this risk. Furthermore, the user must agree to a full wipe of the personally owned device if they leave. This may result in the loss of both company and personal data on the device.

No liability is accepted by McSence for any use of personally owned devices for which users remain fully responsible at all times.

**Lost or stolen devices:** Devices that fall outwith the control of the organisation represent a risk to data and cyber security. Any McSence owned devices or other devices that have been connected to the McSence network which are lost or stolen or are otherwise outside the control of the authorised holder must be reported to the Chief Executive or the IT Support Contractor immediately.

On receipt of confirmation of a missing device, the IT Support Contractor will arrange to have this barred from connecting to the network until if it recovered or permanent loss is confirmed. The company also maintain remote access and remote data wiping capabilities for all McSence owned devices and depending on the circumstances the Chief Executive may authorise devises to be remotely wiped to protect company data and access to our systems.

**Data Recovery:** The company follows the principles of 3-2-1 data backup and recovery. Each of the company's servers backs up to the other to provide a copy of all data off site. We also take a further backup to the cloud, so the data is maintained off site and on a separate media. Our Microsoft 365 email data is also backed up and protected by a proprietary cloud product offered by Arcserve.

If staff become aware they may have inadvertently lost or misplaced data, it may be possible to recover this and a request to do so should be made to the IT Support Contractor at the earliest opportunity.

**Departing Staff:** When staff leave employment with the Company, the Business Unit Manager will be responsible for ensuring all IT equipment and devices in their possession are returned and are in working order. If necessary, devices can be deactivated remotely and if this proves necessary the Business Unit Manager must advise the Chief Executive or the IT Support Contractor accordingly as soon as reasonably practical.

The Business Unit Manager should advise the Chief Executive of all staff leaving and the leaving date so access to the company's network and system can be closed. In some instances, it may be necessary to restrict access to the Company's network immediately on notice of resignation or termination rather than waiting until the leaving date in which case the Business Unit Manager must advise the Chief Executive immediately.

All returned company devices should be passed onto the Chief Executive for reallocation. Any internal reallocation of equipment between staff authorised by Business Unit Managers must be reported to the Chief Executive who will update the IT asset register accordingly.

All accounts for departing staff will be blocked in the first instance to allow Business Unit Managers to determine what data needs to be kept and transferred. This exercise must be completed as soon as possible and at worst 30 days after departure and the Chief Executive informed when the account can be deleted.

**Administrator Access:** Administrator access to McSence systems, networks and equipment will be strictly limited to the Chief Executive and the IT Support Contractor only. All actions requiring administrator action will be carried out by the IT Support Contractor. Under no circumstances should administrator passwords be passed to members of staff to carry out administrator actions themselves. The Chief Executive will be issues with a separate administrator logon and password to ensure there is not a constant administrator access route open on the network.

**Abuse of The Policy:** If employees become aware of a breach of this policy or an incident that could lead to a breach, they must report this immediately to their Business Unit Manager or in their absence, directly to the Chief Executive.

Similarly, any employee who becomes aware or suspects that their account may have been compromised, must report this immediately as above.

The company holds Cyber Protection Insurance which can help us to recover from any breaches but to take advantage of this we must make a referral to the Insurance Company at the earliest possible opportunity. This will be done by the Chief Executive or in his absence, his authorised deputy.

**Training:** The Business Unit Manager will assess all staff joining and those changing job roles internally for competence in IT aspects of their role and record this on the Training Matrix for their department. Any training needs identified should be carried out as soon as possible in conjunction with the Training team. The company will provide training in the application of this policy and also some general cyber-security training as part of the induction process for staff joining with an IT role to play.

Any staff who feel they need additional training in any aspects of this policy should raise this with their Department Manager either immediately they become aware or at their next regular performance review meeting.

**Feedback:** The Company are keen to engage with all stakeholders regarding policy or procedural matters at any time and all feedback regarding this policy including issues with compliance or areas where it could be improved would be most welcome. These should be directed to the Business Unit Manager or directly to the Chief Executive.

---

**Company Intranet – Staff Zone:** All the McSence Groups policies, procedures, handbooks are available on-line to all employees on the McSence Group's Staff Zone Intranet via our website Login | McSence

**Compliance:** Failure to comply with the provisions of this Policy may result in Disciplinary proceedings.

*McSence Group Signatory:*
**David Maxwell | Chief Executive**
**McSence Group** - *McSence Communication Ltd, McSence Ltd, McSence Services Ltd & McSence Workspace Ltd*
**T: 0131 454 1500 | E:** mail@mcsence.co.uk **| W:** www.mcsence.co.uk **| FB:** www.facebook.com/McSenceGroup

***Policy Amendments & Revisions:*** *This policy will be reviewed annually and, if necessary, revised in the light of legislative or organisational changes Improvements will be made by learning from experience and the use of an established annual review. Should any amendments, revisions, or updates be made to this policy it is the responsibility of the Company Senior Management Team (SMT) to see that all relevant employees receive notice and training if necessary.*