SOCIAL MEDIA & IT COMMUNICATIONS POLICY

Policy Statement: The McSence Group IT communications are a key part of our business, and so it is crucial that we adhere to certain standards to protect all parties. This policy sets out our current rules, guidelines, and procedures for IT use. This policy applies to all employees, including those who work from home or remotely, but also to any other individuals using our systems. New employees should be made aware of its content upon joining us as part of the induction process.

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:

- 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: The purpose of the policy to confirm that at all times, our IT systems and associated facilities are primarily a business tool and that the electronic transfer of data is an important part of our operations. We aim to take a fair and consistent approach to IT usage within the business. Therefore, this policy sets out our rules on email, social media, and internet use, and what we would deem to be both appropriate and inappropriate use.

Users who believe they have violated these policy requirements, or who become aware of misuse or violation by others should report the facts to their Line Manager immediately. We require all users not to cause offence to others or cause an obstruction or knowingly introduce any form of computer virus or malware to our IT systems.

Legal Considerations: McSence Group also has a regulatory responsibility to ensure that client and staff data is held by us safely and securely in line with Data Protection and General Data Protection Regulations (GDPR). The following pieces of legislation apply to this policy:

- The Interception of Communications Act 1985
- The Computer Misuse Act 1990
- The Health and Safety (Display Screen Equipment) Regulations 1992
- The Protection from Harassment Act 1997
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Data Protection Act 2018
- General Data Protection Regulations (GDPR)
- Any Codes of Practice issued from time to time by the Information Commissioner's Office (ICO)

System Security for Computers, IT Equipment and Social Media Procedures: Individual users are responsible for the security of their IT equipment and must not allow this to be used by an unauthorised person. Personal password(s) should be kept confidential, and all reasonable precautions taken to prevent unauthorised access to the data stored on our equipment and on our network.

Passwords: Passwords should not be disclosed to anyone not authorised to have these and should not be written down anywhere where they could be easily retrieved by someone else. Passwords may be changed from time to time, especially when someone leaves our employment. Users should never use another person's email address or password, nor should they permit any other person to transmit, download, copy, forward or store material using their email address or password.

The minimum password requirements are **8 characters with at least 1 number and 1 upper-case/capital letter**.

When logged onto our system, and when leaving any IT equipment unattended, or on leaving our workplace, users should ensure they log off the system to prevent unauthorised access. Any printed material should also be collected and stored confidentially. All users are responsible for ensuring that any information saved onto a local computer or local drive(s) is kept to the absolute minimum.

Our IT technology should be used responsibly, and in a way that does not interfere with, disrupt, or prevent anyone else legitimately using these resources. Users should ensure they are aware to which drives they have access/modification rights and remember this when saving confidential data. This is to make certain that the right people are able to view and edit the files saved to the system.

Unauthorised access, attempts to access, modify, delete, or use data belonging to McSence or programs will be considered a disciplinary matter and potentially a criminal offence under the Computer Misuse Act 1990.

The licence agreement that accompanies software packages should be strictly adhered to. Unauthorised copies of software should not be made for use within the office or outside. Equipment allocated to individuals will be supplied with the appropriate software and configuration. Users are not permitted to load screensavers/software from any source without the prior permission of your Line Manager.

On leaving our employment, access to our systems will be immediately withdrawn. Incoming emails will be diverted to the leaver's manager and an automatic response will be set up informing the sender that the address is no longer to be used to contact the leaver. Any passwords giving remote access to our systems will be changed, thus preventing unauthorised access. We will also notify any suppliers or contractors of any leavers who should be removed from their list of those who are authorised by us to use their services. Note that in order to protect our business interests, the above may also apply during any period of "garden leave".

Portable Equipment: Portable equipment should not be left unattended when away from our premises and should never be left in parked vehicles or unattended at client/customer premises. It is particularly emphasised that our back-up procedures specific to portable equipment should be followed at all times. It is important to ensure all portable devices are protected with suitable security in the event that they are lost or stolen. All portable equipment that holds company data including emails, documents and files must be protected with a PIN code at all times. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disabled or removed.

If an item of portable equipment is lost or damaged this should be reported to your Line Manager. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the excess currently in force with the company's insurers for loss or damage to company property.

In order to protect confidential information, unless it is a requirement of your job and this has been authorised, it is forbidden for photographs or videos to be taken in the workplace, without the prior written permission of the homeowner, landlord, customer and/or client. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still. Unauthorised photographs or videos found to have been taken by staff will be deemed gross misconduct, and the staff member liable to dismissal.

Under no circumstances should any meeting or conversation be recorded without the permission of those present prior the commencement of the meeting or conversation. In addition, we do not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for business purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from your Line Manager.

Email: Our email facilities are intended to promote effective and speedy communication on work-related matters. On occasions it will be quicker to action an issue by a phone call, texting, or face to face, rather than via protracted email chains. Employees are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

All office-based employees who need to use email regularly as part of their role will normally be given a McSence Group business email address and account. If anyone who does not already have access believes that there is a genuine job requirement, a written request should be made to your Line Manager, setting out the business justification. We may, at any time, withdraw email access to any employee, should we feel that this is no longer necessary for the role or that the system is being abused.

Emails are merely another form of communication: in some instances, they may be the only contact that a recipient has with the McSence Group and the style, appearance and content of the email will therefore influence the image that is portrayed of our businesses. Emails appear to be a more informal type of communication, but our normal standards of presentation and content apply equally to them and the language used in the message must be professional. This includes spelling, punctuation and correctly heading each email as appropriate. All emails sent externally must include our name, address, contact telephone number, details of our company and charitable status and our standard disclaimer.

- Email messages should be concise and directed only to those on a 'need to know' basis. General messages to a wide group should only be used where necessary.
- Long email trails should not be sent unless absolutely necessary and messages should only be marked as 'urgent' if they warrant immediate action. “Read receipts” and requests to “acknowledge acceptance” of an email further add to email traffic, so should not be set-up as automatic. Staff are to be mindful of the size of attachments within emails. Very large attachments can have an impact on speed and performance of the email systems and internet connections. Where possible, the size of pictures should be reduced, and very large files compressed into smaller files by using the “zip” function.
- Confidential information must only be sent to an authorised person(s) and should not be sent externally by email without authority. Such messages should be fully encrypted (or any attachments containing confidential information password protected and the password sent separately).
- Messages sent by email can give rise to legal action against us. Claims of defamation, breach of confidentiality or contract could arise from a misuse of the system. Emails should therefore be treated like any other form of correspondence and, where necessary, hard copies retained. Statements should not be made in an email which could, intentionally or otherwise, create a binding contract or make a negligent statement. Neither should opinions or views be expressed that could be interpreted as misrepresenting our products, services, or those of any other organisation with whom we deal.
- Emails should not be transmitted, copied, or forwarded to third parties without the sender's permission.
- Emails, however confidential or damaging, may have to be disclosed to third parties and messages are disclosable in any legal or regulatory action commenced against us relevant to the issues set out in the email. Even deleted emails may still be recoverable and are regarded as legitimate forms of evidence in court.
- All email messages are the property of McSence and are treated as records of the business.
- Emails should be checked regularly, and employees who are away from their place of work for more than a day should ensure that an appropriate message is sent automatically to senders and/or that temporary access is granted to another colleague and that emails are dealt with in their absence as appropriate. With the exception of senior managers, unless specifically requested to do so, employees are not expected to read or action their emails when on any form of leave.
- During unplanned leave or prolonged absence, and solely where necessary, we may access and/or divert email accounts in order to continue the smooth operation of our business.
- Anyone who receives an email message that has been wrongly delivered to his/her email address should notify the sender by returning the message to that person. If the message contains confidential information, this must not be disclosed or used.
- Our email system should not be used for spreading gossip or nuisance mail, for personal gain or in breach of any of our employment policies, such as equal opportunity, bullying or harassment. Sending unwanted, abusive, discriminatory, or defamatory emails can constitute bullying or harassment and will be treated as a serious disciplinary issue. This also applies to any emails sent from personal equipment to work colleagues or other contacts of McSence.
- Take care before sending or viewing material which may be of a hurtful, suggestive, or harassing nature: it is the view of the recipient that determines whether it is inappropriate, even if the recipient was not the original addressee. Any emails that contravene this policy should be brought to the attention of your Line Manager immediately.

- All email footers must not deviate but exactly follow the McSence Group's brand guidelines with GDPR compliant footers.

Internet Use: Utilising the vast amount of data that can be found on the Internet can be a useful resource and may be integral to some roles within our business. All employees who need to use the Internet as part of their role will normally be permitted access. If anyone who does not already have access believes that there is a genuine job requirement, a written request should be made to the Business Manager, setting out the business justification. We may, at any time, withdraw Internet access to any employee, should we feel that this is no longer necessary for the role or that the system is being abused.

Having access to the Internet demands a level of trust and responsibility, as websites visited will record the computer system's IP address. This is one of the main reasons we ask that users should restrict their access to websites necessary to complete their daily tasks and not to access any other sites for personal use. Many sites require registration. If there is any doubt as to whether it is appropriate to register as a user of a website for work purposes, users should check with your Line Manager.

In general, information should not be sent or received via the Internet unless the transmission is both legal and secure. If in doubt, check with your Line Manager.

Personal Use of IT systems: McSence Group's IT, Email, company landlines and mobile phones are provided for business use, and although it is accepted that occasionally private use including but not limited emails, web browsing, calls and texts will be sent/received, this should be kept to a minimum and agreed in advance with the Line Manager. It should be clearly understood that whilst we do not routinely monitor messages, we do reserve the right to monitor and to access any incoming or outgoing messages within our email and phone systems. Company mobile phones should not be used to make personal calls, except in unavoidable emergencies and it should be reported when this occurs. Messages may be read by other people and therefore anything of a strictly private or personal nature should not be sent or received using our email system.

The Internet may be accessed for personal use during working time. Personal use of the Internet, and the loading, sending, or viewing of pornographic, non-licensed, suggestive, obscene, or offensive material is not acceptable and will lead to disciplinary action, including dismissal as a possible outcome.

Our systems may not be used for any of the following, this list is not exhaustive but indicates the sort of usage we would consider to be unacceptable, and which may lead to disciplinary action, including dismissal as a possible outcome:

- Gambling
- Downloading, accessing, or storing large personal files which interfere with the running of the organisation, such as photographs, videos, and music
- Games of any kind
- Copying software for personal use or using our software (including accounting programs and/or design programs) for personal use
- Promoting non-business related religious, charitable, or political material with the intention to solicit (unless authorised)
- Sending or participating in junk mail, spam mail or chain letters (this includes forwarding jokes, cartoons, and video clips to groups of people, and also transmitting unsolicited commercial or advertising material that is not work-related)
- Bringing our name into disrepute via social networking websites
- Undertaking deliberate activities that waste staff effort or networked resources
- Using the McSence email address and misrepresenting McSence
- Using our name, business contacts, clients or customers for personal benefit or the benefit of any other firm, company, or organisation

We also have an office-based wireless network and using a portable device to make personal Wi-Fi hotspots which bypass our existing Wi-Fi is not allowed.

System Monitoring: Internet, email and computer usage is continually monitored as part of our IT protection against computer viruses, our ongoing maintenance of the system, and when investigating faults.

Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

We reserve the right to monitor all incoming and outgoing emails. This will normally occur in circumstances where we suspect the viewing or sending of offensive or illegal materials; discriminatory comments or those detrimental to the business; or excessive personal use of our IT and email systems. When monitoring emails, we will, in most cases, restrict this to the address and heading of the emails. Personal emails should be clearly marked as such, and where possible we will avoid opening these unless there is a suspicion of improper use and they form a relevant part of a disciplinary investigation.

We have in place content controls and filters to prevent inappropriate Internet use but reserve the right to monitor all Internet usage. Again, this will normally occur where we suspect the viewing of offensive or illegal materials, or an excessive amount of time spent viewing non- work-related websites. Excessive use of Records, emails and/or Internet usage and sites visited will normally be retained for a period of one year.

Computer Viruses: Unknown files or messages must never be introduced into the system without first being checked for viruses. ALL incoming material should be checked for viruses, whether loaded manually (e.g., from CDs or memory sticks) or transmitted from an external source such as the Internet. Any problems relating to viruses should be reported immediately to your Line Manager. Personal CDs, disks or memory sticks should not be used on our computers under any circumstances.

Emails from unknown sources should not be opened - this is how most viruses are introduced and they could easily spread throughout our systems. 'Junk mail' should not be responded to, nor mass warnings distributed regarding new email viruses. Chain letter-type mail should also not be responded to nor forwarded. All such emails if received must be deleted without opening them. Particular care should be taken when opening attachments, and should any attachment produce strange or unexpected results, your Line Manager should be notified immediately.

Remote Working: Increased IT security measures apply to those who work away from their normal place of work (e.g., travelling, working from home or at a different venue) or who are working in clients' homes. When working in a client's home, do not log in to the internet, make personal calls or log in to a Wi-Fi hotspot.

If logging into our systems or services remotely, using computers or other devices that either do not belong to us or are not owned by the user, any passwords should not be saved, and the user should log out at the end of the session deleting all logs and history records within the browser employed. If this is not clear for the particular configuration of kit (for example at an Internet café), our services should not be accessed from that device.

The location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc.

- Any data printed should be collected and stored securely
- Files should be password protected and data saved to our system/services when accessible

Those issued with a 'dongle' to enable Internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should note that the cost of Internet access can be very high. Dongles should therefore be used for essential business purposes only, especially if abroad. Similarly use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential business use.

Accessing McSence's server by staff using their own smartphones, tablets, laptops without permission and/or agreement with the immediate Line Manager is not allowed. If this is found to have happened, the staff member will be liable to disciplinary action.

Social Media: Social media includes blogs or other similar sites where text can be posted, multimedia or user generated media sites (YouTube), social networking sites (such as but not limited to, Facebook, LinkedIn, Twitter, Instagram, Snapchat, TikTok, Ning or Myspace), virtual worlds (Second Life), text messaging and mobile device communications such as Snapchat and Instagram and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either via our systems or from home.

Inappropriate comments can adversely affect the reputation of our organisation, even if it is not directly referenced. It should be noted that if comments/photographs are likely to be construed as linked to the McSence Group, or, in more direct cases, if comments about colleagues, clients/customers or our business could be regarded as abusive, humiliating, discriminatory or derogatory, or could constitute bullying or harassment, we will treat this as a serious disciplinary offence. In addition, postings to websites should not breach copyright or other law or disclose confidential information, defame McSence, its suppliers, clients/customers, or employees, or disclose personal data or information about any individual that could breach the Data Protection Act 1998 & 2018.

McSence does not encourage employees to write about their work in any way and would prefer them not to do so. If individuals choose to do so they should not disclose our name nor allow it to be identified by any details at all. Employees should be aware that competitors or other organisations may read employees' personal weblogs, to acquire information on, for example, their work, products, technical developments, and employee morale. Therefore, even if McSence is not mentioned, care should be taken with any views expressed. If something is not public information, it should not be shared. In particular, the following must not be posted on social media:

- Photos, videos and/or sound recordings taken on our property, unless explicit written permission has been given by your Line Manager to do so
- Photos or videos showing any employee or workers in McSence Group's uniforms or other clothing that includes our logo and that could reflect negatively on the employee, their job, their colleagues, or the McSence Group
- Details of any kind relating to any events, conversations, materials, or documents that are meant to be private, confidential, or internal to the McSence Group. This includes but not limited to manuals, policies and procedures, training documents, emails, work rota/rosters, client registers/information, sales databases, non-public financial or operational information, personal information regarding other employees or clients/customers/suppliers, anything to do with a disciplinary case, grievance or legal issue, product specifications, any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements
- Any contact relating to a posting that concerns the business of the McSence Group should not be responded to and should be referred to your line Manager.
- Even if McSence Group is not mentioned, care should be taken with any views expressed and any views should clearly be stated to be the writer's own (e.g., via a disclaimer statement such as: '*The comments and other content on this site are my own and do not represent the positions or opinions of my employer.'* Writers must not claim or give the impression that they are speaking on behalf of McSence.

We may from time to time monitor external postings on social media sites. Any employee who has a profile, for example on LinkedIn or Facebook, must not misrepresent their role with us. Employees are also advised that social media sites are not an appropriate place to air business concerns or complaints. These should be raised with the Line Manager or formally through our grievance procedure.

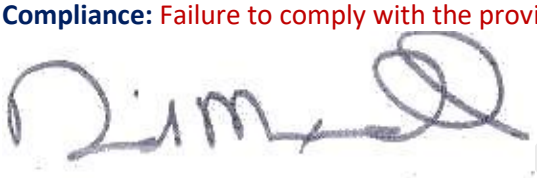
If, however, an employee is asked to contribute to an official weblog on behalf of the McSence Group then the specific details will be discussed at the time. If writing any such weblogs, employees will normally be asked to state that any personal views expressed do not necessarily reflect the views of McSence. Links to our website are not allowed without the consent of your Line Manager. In summary, the guidance has to be: *'If in doubt, check and always think through possible consequences before you post, text or discuss anything on social media.'*

Company Website: The McSence Group has a specific website managed and updated by the Group Business Development Manager. Employees should not post on the Group's website without authorisation. Employees should refrain from creating a link to the website in any social media communication they may undertake as individuals. If the employee feels it would be of advantage to link our website to another website, they should raise this with the Group Business Development Manager in the first instance.

Termination or Resignation of Employment: Our clients'/customers' contact details, personal and sensitive information remain the property of the McSence Group. Upon leaving our employment, for any reason, direct contact from our existing or prospective clients/customers should be directed to your immediate Line Manager or Business Unit Manager and any contacts gained whilst in our employment (including those on LinkedIn or any other networking platform) should not be used for any purposes that may be in competition with us. In addition, employees leaving the McSence Group will be required to delete all work-related data including client/customer contact details from any personal device or portable equipment. The Group Operation's Manager has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes to our working practices. Any breach of this policy will be treated as a disciplinary issue and dealt with through our disciplinary procedure.

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.*