CONFIDENTIALITY POLICY

Policy Statement: During your employment with the McSence Group you may have access to a wide range of confidential information, and sensitive data where it may not always be obvious to you that it is confidential. McSence Group needs to collect and use certain information about customers to allow us to carry out our many and varied functions and responsibilities. This personal information and/or sensitive data – however it is acquired, held, processed, released, or destroyed – must be dealt with lawfully and properly, and McSence Group of companies will work within the terms of the Data Protection Act 1998 (the Act) which also incorporates the changes on 25th May 2018 with the General Data Protection Regulation (GDPR) in all its dealings with personal data.

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".

Sensitive Data: Do seek advice from your Line Manager if you are not sure about the sensitivity of any information that you have access to. Sensitive personal data is also covered in GDPR as special categories of personal data and the special categories specifically include:

- Genetic data relating to the inherited or acquired genetic characteristics which give unique information about a person's physiology or the health of that natural person.
- Biometric data for uniquely identifying a natural person, including facial images and fingerprints.
- Data concerning health which reveals information about your health status, including both physical and mental health and the provision of health care services.
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sex life or sexual orientation

Under existing and new data protection rules, GDPR, anyone who processes personal information must make sure that the information is (amongst other things):

- Adequate, relevant, and not excessive
- Processed fairly and lawfully.
- Obtained only for one or more specified and lawful purposes, and not further processed in any manner incompatible with that purpose or those purposes.
- Accurate and up to date
- Processed in accordance with the rights of data subjects under the Data Protection Act
- Kept for no longer than is necessary.
- Secure (i.e., using appropriate technical or organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data)

You must not directly or indirectly pass onto a third party, including colleagues, any confidential information that is given to you, or to which you have access, without authority from the Company. In addition to any information marked confidential or secret, all commercially sensitive information including sales, margin and profit figures, forecasts, plans, promotions, new product developments, computer programs, potential acquisitions etc, is considered confidential as is information regarding other employees, customers or suppliers and the security of employees, premises, merchandise, cash, and vehicles.

Any company information held by you includes but not limited to "personal and company smartphones; laptops; computers; tablets; netbooks; iPads, organisers, handheld or similar devices that have email and/or internet capability to access our system that is owned by the company or you, must be deleted prior to the termination of your employment.

Documents, files, and other items may be removed from the Company's premises only with the prior authority of your Line Manager or the Senior Management Team (SMT) depending on the reason for requiring access. All such documents, including any copies taken, must be returned at the date/time specified when gaining prior authority and when you leave employment from the Company. Employees, who are authorised to take information off-site in any form, should ensure that they are conversant with the Company's Data Protection Policy and GDPR.

You must not, either during your employment or at any time thereafter:

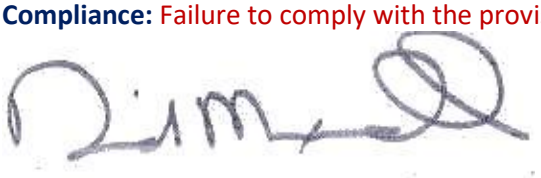
- Divulge any of the confidential business affairs or finances of the Company or its dealings, transactions, or affairs to any other persons without the previous consent in writing of the Company.
- Publish or issue any book, article, or note relating to any of the products or services of the Company without having obtained the prior approval in writing of the Company.
- Use or attempt to use any information relating to the business processes or methods of the Company, except in the performance of your duties to and for the benefit of the Company.

Do seek advice from your Line Manager or the Senior Management Team (SMT) if you are not sure about the sensitivity of any information that you have access and to. If you have any concerns regarding breaches in the Company Confidentiality Policy you or others including colleagues and/or third parties, it is your responsibility to raise your concerns in writing, email is acceptable, with your immediate Line Manager or where that is not appropriate, the Senior Management Team (SMT).

A breach of any of these rules may result in summary dismissal. You are bound by law not to reveal any confidential information about the Company after you leave. Some employees may be subject to other contractual conditions regarding confidentiality if the nature of their role gives them access to particularly sensitive or confidential information. Please refer to your Statement of Principal Terms and Conditions.
This clause of your contract is without prejudice to your common law duty of confidentiality. It does not override your entitlement to protected disclosures under the Public Interest Disclosure Act. The Company will respect your right to confidentiality and all information regarding you will be held in compliance with the Data Protection Act 1998.

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.*