GDPR & DATA PROTECTION POLICY

Policy Statement: A guiding principle for McSence Group in conducting its business is the protection of the fundamental rights and freedom of individuals and their right to privacy with respect to the processing of personal data. 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 – however it is acquired, held, processed, released, or destroyed – must be dealt with lawfully and properly, and McSence Group 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".

General Data Protection Regulation (GDPR): governs your personal data rights, including the way companies handle data and the compensation individuals can claim for misuse of their data. The General Data Protection Regulation is a set of EU-wide data protection rules that have been brought into UK law as the Data Protection Act 2018. When consumers buy goods and services, or sometimes even just visit a website, the organisations may collect information and data about the consumer. This might include name, address, and date of birth. This type of data, which can identify a living individual, is called 'personal data'. Organisations may even include things like the schools, jobs, partner or family or the sorts of things viewed or bought online where many organisations, including councils, hospitals, travel companies, banks and supermarkets hold data about individuals.

Responsibility: McSence Group has a corporate responsibility for data protection and is defined as the "Data Controller" by the Act.

McSence Group has established a **Senior Management Team (SMT**) whose remit includes considering and advising on personal data management issues affecting McSence operations. The SMT plays an important role in ensuring McSence follows best practice in complying with the Act. To support the SMT each Business Unit Manager is the nominated Information Management Officer or officers whose role shall be to promote best information management practice within their division and to attend meetings with the SMT. This policy applies to all divisions, staff (including agency staff), and elected members of the group where it covers all the personal data, as defined in the Act, which McSence processes.

The **Chief Executive** will provide the overall lead in relation to data protection matters and will be the member of the Senior Management Team (SMT) accountable for information management within McSence Group to ensure that compliance with the Act and best practice can be demonstrated.

The **Group Operations Manager** will be the McSence Senior Information Risk Owner. Each Business Unit Manager will retain executive authority for compliance with the Act within their Division and each Head of Service will be responsible for ensuring that their service's information and systems comply. Each Head of Service will be required to

nominate an appropriate information Management Officer to act as data protection officer for their Service. Their main role will be monitoring compliance within their Service, in passing on advice and training, in maintaining the accuracy of their Service's input into the McSence notification and processing subject access requests which relate to records from their Service. The Head of Customer Services will maintain an up-to-date list of these officers.

While McSence Group is not obliged to record every individual filing-system that holds personal details, the Chief Executive will maintain an internal Register of Systems that perform that function. The Register will be useful for two purposes. Firstly, quickly, and easily identifying all possible repositories of information about a data subject if a data subject access request is made and, secondly, ensuring that good practice is followed in the custody and maintenance of data. The Register will also allow the nominated member of staff who is the 'owner' of a filing system to record personal details. The Register will also contain details about the accuracy of data. Once a year the Chief Executive will ask the 'owner' to review the accuracy of the entries in the Register. Information on the Register will be made available on the intranet.

All Employees are individually responsible for ensuring that their collection, storage, processing, and destruction of data is in accordance with the Act. Where appropriate, training and guidelines will be provided. The Act applies to McSence acting in their capacity as an elected member of the McSence Group or on a Committee of McSence.

Elected members will only be given access to personal data when knowledge of the content of such data is necessary for them to undertake their McSence responsibilities. They will be provided with access to personal information only in compliance with the provisions of the Act and the eight data protection principles, or when the relevant data subject has authorized the access in writing. Personal data disclosed to elected members will remain the property of the McSence Group and cannot be used or disclosed for purposes other than those for which it was provided.

Sensitive Data*:* Sensitive personal data is also covered in GDPR as special categories of personal data. 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)

Advice and Training*:* The McSence Principal Solicitor will offer legal advice on data protection and privacy issues as and when they arise. The Principal Solicitor will also arrange, if considered necessary, training for officers in the form of seminars tailored to suit the needs of their individual service or section.

Notification: The Act requires that all data controllers notify their holdings of personal data held in computerised form to the information Commissioner. The Group Operations Manager will be responsible for establishing and maintaining the McSence Group's notification. The appropriate Business Unit Manager in each department will be responsible for reporting changes in processing to the Group Operations Manager after consultation with the Principal Solicitor. Procedures have been developed to ensure that the McSence notification is accurate. where there is no requirement to notify personal data held in structured manual files, although these are covered by most of the other provisions of the Act. The information Commissioner maintains a public register which details:

- The name and address of the data controller, and a contact for enquiries.
- A description of the personal data and of the categories of subject to which it relates; and A description of any recipients to whom the data may be passed.

Data Subject Rights: The Act grants data subjects' certain rights in relation to that data. These include the right to prevent processing likely to cause damage or distress, or to prevent processing for direct marketing, they also have the right to act if they feel that they have been damaged by a contravention of the Act by a data Controller. They can have inaccurate data rectified, blocked, or erased, and can request that the information Commissioner carries out an assessment of a data controller's processing of their data. Data subjects also have the right of access to data held on them. The Group Operations Manager has overall responsibility for ensuring that the rights of data subjects access request. The Group Operations Manager will also keep under review detailed guidelines on dealing with data subject access requests and will have overall responsibility for processing cross-divisional requests. Those relating to only one division will be the responsibility of that division, subject to any guidance from the Principal Solicitor. Normally, McSence will charge the maximum statutory fee of £10 for processing a data subject access request.

Data Retention: McSence Group will develop comprehensive retention schedules. These will cover all records in each division and will define how long data is to be retained, thus ensuring compliance with the Act's fifth principle. Each Business Unit will create a Retention Schedule following consultation with the Records Officer, after examining their own records. The Retention Schedule should be compiled about relevant legislation and best practice both with McSence and elsewhere. The Schedules will be created and maintained by Divisional administrators and signed off by the appropriate Head of Service and will then be binding on all staff. A copy of each up-to-date Retention Schedule will be supplied to the Records Officer.

Security: All officers will be responsible for following procedures and systems for maintaining appropriate security of personal data to which they have access, those detailed in the McSence Information Security Policies and Guidelines, the Records Management Guidelines, and in the Data Protection Guidelines.

Freedom of Information: McSence Group in committed to open and transparent Government and to meeting its responsibilities under the Freedom of Information (Scotland) Act 2002 (FOISA). McSence has a procedure for complying with FOISA in relation to the provision of information and the conduct of reviews of decisions whenever requested. Where there appears to be a conflict between an individual's right to privacy and the public's right to know this should be referred to the relevant Information Management Officer in the first instance, failing whom the Principal Solicitor.

GDPR Data Policy & Breaches: McSence personal information – however it is acquired, held, processed, released, or destroyed – must be dealt with lawfully and properly, and McSence Group 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. GDPR introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. You should ensure you have robust breach detection, investigation, and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals. You must also keep a record of any personal data breaches, regardless of whether you are required to notify. In respect of employees, a breach of this policy may be dealt with under the McSence disciplinary Procedures. Individuals could also be prosecuted for unlawful action under the Act.

Checklist 1: Preparing for a personal data breach.

- ☐ We know how to recognise a personal data breach.
- ☐ We understand that a personal data breach is not only about loss or theft of personal data.
- ☐ We have prepared a response plan for addressing any personal data breaches that occur.
- ☐ We have allocated responsibility for managing breaches to a dedicated person or team.
- ☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Checklist 2: Responding to a personal data breach.

- ☐ We have in place a process to assess the likely risk to individuals as a result of a breach.
- ☐ We know who the relevant supervisory authority for our processing activities is.
- ☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- ☐ We know what information we must give the ICO about a breach.
- ☐ We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
- ☐ We know we must inform affected individuals without undue delay.
- ☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- ☐ We document all breaches, even if they do not all need to be reported.

Information Commissioner's Office (ICO) & Scottish Public Services Ombudsman Contact Details:

A breach of this Policy by an employee of McSence Group or an elected member may have serious consequences for McSence Group and may be the subject of a complaint to the Information Commissioner and/or the Scottish Public Services Ombudsman – For any alleged data protection breaches should be referred to the following quoting Ref ZA033228:

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire, SK9 5AF
T: 0303 123 1113

Scottish Public Services Ombudsman
Bridgeside house
99 McDonald Road
Edinburgh, EH7 4NS
Freephone 08003777330
T: 0131 225 5300 (this contact information collected by SMC from the SPSO.org website)

About elected members a breach of this policy may be subject to McSence internal complaints procedure and to a complaint to the Standards Commission. Elected members could also be prosecuted if a criminal offence has been committed or for unlawful action under the Act. Details of the Standards Commission is shown below:

Standards Commission for Scotland
Room T2.21,
Scottish Parliament,
Edinburgh,
EH99 1SP
T: 0131 348 6666
E: enquiries@standardscommission.org.uk

Audit: Consideration will be given to the provision of an ongoing audit regarding data protection, periodically checking security systems, adherence to retention schedules and the accuracy of the McSence notification.

Data Protection Principles:

Data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant, and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights secure
- Not transferred to countries without adequate protection

Basic Guide to Data Protection – DO:

- ✓ Check identity of person asking for information
- ✓ Update and correct records as soon as possible
- ✓ Log out before leaving your screen unattended
- ✓ Forward all subject access request forms/letters to Director, Corporate Services
- ✓ ASK YOUR SUPERVISOR if you have any doubts or problems
- ✓ Contact Legal Services if you have any legal queries

× **Basic Guide to Data Protection – DON'T:**

- × Disclose information to any unauthorised person
- × Disclose your password to anyone
- × Use PC, Laptop, tablet, VDU, or phone for displaying confidential data when your terminal screen might be seen by members of the public or other unauthorized person
- × Leave input documents or printouts lying out: file or store them out of sight
- × Dispose of person/confidential data carelessly shred it

Data Protection Act Guidelines: The guidelines below give more detailed information about data protection, including a few examples. If anything is still unclear, ask your line manager or contact Group Operations Manager. Under the Data Protection Act 1998 (the 'DPA'). McSence must register with the office of the Information Commissioner and give general descriptions of all the personal data held by it gets the data and all the persons to whom it may wish to pass on the data. McSence must ensure that personal data is processed in accordance with the terms of the DPA.

What is Personal Data? Personal data is information held on a relevant filing system, which includes data held manually or electronically, that relates to a living person and identifies an individual either expressly or by implication. For example, even if the data does not include the name and address of the person, it would still be personal data if it included their National Insurance Number and the McSence separate lists of these numbers showing each person's name against his number. The GDPR adds in a new range of personal identifiers, reflecting changes in technology and the way companies gather data today. Online identifiers, such as IP addresses, are now included within the definition of personal data. Personal data is information that relates to an identified or identifiable person who could be identified, directly or indirectly based on the information. For example, name, address, and date of birth were all already considered personal identifiers under the Data Protection Act 1998. Personal data is now regulated by the Data Protection Act. The EU-wide General Data Protection Regulation (GDPR), brought into UK law on 25 May 2018 under the newly revised Data Protection Act 2018, broadened the definition of what counts as personal data. Personal data includes an identifier such as:

- Name
- An identification number, such as your National Insurance or passport number
- Location data, such as home address or mobile phone GPS data
- An online identifier, such as your IP or email address

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 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)

What is Processing?: The definition of processing in the DPA is very wide and covers obtaining, recording or holding information or data: carrying out any operation or set of operations on the information or data including: Organisation, adaptation, or alteration; retrieval consultation or use; disclosure by transmission, dissemination or otherwise making available or alignment, combination, blocking, erasure or destruction, the definition covers just about everything that can be done with data.

Offences*:* Subject to certain exemptions it is an offence for McSence Group or employees to process personal data without registering it with the Information Commissioner. McSence employees can be disciplined if they deliberately or recklessly misuse personal data and, in extreme circumstances, can themselves be criminally liable. However, if employees process personal data fairly and sensibly, and ask for advice when in doubt, there should be no difficulties.

Principles*:* There are eight basic DPA principles. Personal data must be:

- Obtained and processed fairly and lawfully (e.g., the person giving the information is entitled to know the reason for which the information is being collected)
- Held only for the lawful purposes described in the Register (e.g., if data is used for a completely new purpose, this should first be registered)
- Adequate, relevant, and not excessive in relation to the purpose for which it is held (e.g., forms used for collecting information about individuals should be designed to obtain only the information required)
- Accurate and, when necessary, kept up to date (e.g., information should be obtained from reliable sources and any mistakes corrected as soon as they are discovered)
- Held no longer than necessary for the registered purpose (when records have reached the end of their usual life, they should be reviewed and deleted unless there is a good reason for keeping them)
- Made available to data subjects on request (see “Subject Access Requests” below)
- Properly protected against unauthorized access/disclosure or loss/destruction (see “Confidentiality” below)
- Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Subject Access Requests: There is a Subject Access Request when an individual ask whether the data of which he or she is the subject. The request must be in writing. An individual is entitled to have a copy of data processed by reference to that person and a description of the data being processed, the purposes for which it is being processed and of any potential recipients of the data. The data subject is also entitled to any information as to the source of the data where that is available. A standard “Subject Access Application” form, along with guidance for the individual, has been issued to all Divisions, and should be used wherever possible – although the individual can insist on making a request in a letter or in some other written form. A fee of up to £10 can be demanded. If not known to the employee, the individual making the application should provide satisfactory proof of identity (e.g., rent book, driving license, passport, utility bill) or of his authority if acting for someone else (e.g., a Solicitor acting for a client might produce a mandate or similar letter signed by his client, a guardian for a handicapped person might produce a letter signed by that person’s Doctor). The individual should supply enough information to locate his personal data, e.g., if he only wishes to find out personal data held on him regarding his housing benefits payments, he should specify this.

However, he is entitled to ask for details of personal data held on all the relevant filing systems used by McSence. Routine requests for information, such as an individual asking for a copy of his planning application, a person asking for details of his position on the Housing Waiting List or the state of his rent account etc, are not subject access requests although employees should still seek proof of the individual's identity before disclosing such information.

However, all applications for subject access under the DPA, as soon as the enquirer has established his identity or authority and the purpose of his enquiry, should be forwarded immediately to the Director, Corporate Services, who will have 40 days to reply. Copies of all the personal data held on the individual should be supplied as soon as possible by the appropriate Division or Divisions, whether in the form of printouts or typed or handwritten notes. If no personal data is held on that individual, or if all the personal data is subject to one of the exemptions (e.g. disclosure for the purpose of prevention of crime or assessment of tax, or for a legal purpose as when a Court Order requires the disclosure,) a written reply will be sent to the individual advising him that no data is held or that the data held does not include personal data which McSence is required to reveal to him. If McSence cannot comply with the request without disclosing information relating to another living individual who can be identified from that information, McSence need not comply with the request unless satisfied that the other individual has consented to the disclosure. If the information relating to another individual includes a reference to information identifying that individual as the source of the information, McSence should supply so much of the information requested as possible without disclosing the identity of the other individual (e.g., by saying "supplied by Mr X", but McSence may also seek the consent of the other individual to disclose the information. If the other consents McSence must disclose the information although it should be noted that there is no obligation on McSence to seek such consent. However, information may be disclosed without the consent of the other individual if it is reasonable in all the circumstances to comply with the request. In this regard consideration must be given to any duty of confidentiality owed to the other individual; any steps taken to obtain the consent of the other individual, whether the other individual can give consent and any express refusal of consent.

Except in such circumstances, there should be no "editing" of information, although there should be an explanation in plain English of any technical terms or codes used in any printout. A record should be kept of all applications and replies. If appropriate, individuals have the right to have data corrected or erased and to claim compensation of any damage caused by inaccurate data.

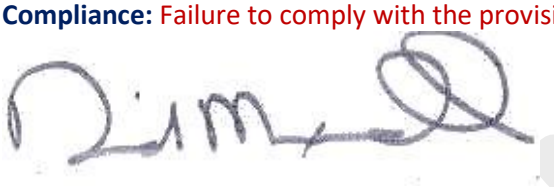
Confidentiality*:* Employees should consult their line manager before processing any new type of personal data or using personal data for a different purpose than before or taking any computers or discs home to perform part of their work (Supervisors may not authorise the removal of particularly confidential data and any such work carried out at home will still make the employee liable to disciplinary action for any misuse or unauthorized disclosure of the data). However, personal data may be disclosed in an emergency if it is urgently required for preventing injury or other damage to anyone's health. Employees should advise their Supervisor if they suspect that there has been any breach of security, e.g., if they believe that some unauthorized person may have learnt their password or tried to log on into their system. Similarly, when logging in, users mask their password and users should never log in in a position where members of the public or other unauthorized persons might see confidential data (e.g., if their PC/Laptop/terminal screens were turned towards a public counter). Screens should not be left unattended when logged into applications. Users should log out if they are not in constant use. Both input documents and printouts should be stored out of sight when not in use, and should be carried in a covered container, such as a box or envelope when being moved between offices. All personal or other confidential data which is to be disposed of should be shredded. Individuals can claim compensation for any damage caused by loss, destruction, or unauthorized disclosure of data.

Register of Systems: While McSence Group is not obliged to record every individual filing-system that holds personal details, please be aware that the Head of Information Technology maintains an internal Register of Systems which performs that function. The Register allows the nominated member of staff who is the "owner" of the system to record personal details. The Register also holds details about the accuracy of the data. The 'owner' of a filing system is asked to review the accuracy of entries in the Register on an annual basis. The Register is useful for two purposes. Firstly, quickly, and easily identifying all possible repositories of information about a data-subject, should a request be made under the DPA and, secondly, ensuring that good practice is followed in the custody and maintenance of data. Information on the Register is available along with detailed guidance relating to the DPA on the Intranet.

Hacking: Under the Computer Misuse Act 1990, computer hacking is illegal and can be punished by heavy fines or lengthy terms of imprisonment. It is a criminal offence to knowingly cause a computer to perform any function with the intention to secure unauthorized access to computer data or a computer programme. It is an even more serious offence to do this with the intention to commit further offences, e.g., theft, or intentionally to cause unauthorized modification of the contents of a computer impairing its operation, hindering access to programs or data, or impairing the operation of programs or the reliability of data, using up spare capacity or corrupting or erasing data (i.e., implanting a 'virus' or 'worm'). The DPA simply provides some protection to the public by recognising the increasing use and sophistication of computerized information and the many possibilities for misuse of personal data. People, who process personal data with reasonable care, bearing in mind the data protection principles, should have no problems. If in doubt about anything, ask your Line Manager or Group Operations Manager.

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.*