MICHAEL LONSDALE
GROUP

DATA PROTECTION AND INFORMATION SECURITY POLICY

MICHAEL LONSDALE GROUP

MLG-POL-000 REV 02 10-01-2023

Contents

Version Control

VERSION	REVIEWER NAME	DATE	NEXT REVIEW	COMMENTS
1.0				

Introduction

The Michael Lonsdale Group inclusive of (Michael Lonsdale Ltd, Michael J Lonsdale Ltd, Michael J Lonsdale (Electrical) Ltd and MJL Midlands Ltd, obtains, keeps, and uses personal and company information (also referred to as data) about clients, job applicants and current and former employees, temporary and agency workers, contractors, interns, volunteers, and apprentices for several specific lawful purposes.

This policy sets out how we comply with our data protection obligations and seek to protect personal and company information relating to our workforce and clients. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal and company information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations, and to being concise, clear, and transparent about how we obtain and use personal and company information relating to our workforce and clients, and how (and when) we delete that information once it is no longer required.

Scope

This policy applies to the Board of Directors employees (full-time, part-time or casual), volunteers and subcontractors of the Michael Lonsdale Group, who will be referred to as ‘staff’ or ‘staff members’.

This document is also applicable to our client's other stakeholders in the Michael Lonsdale Group.

the Michael Lonsdale Group policy and procedure documents may be distributed to clients, suppliers, accreditation, compliance bodies and any other relevant third parties.

In some cases, third parties such as suppliers or those performing on-site work for the Michael Lonsdale Group will be expected to adhere to our policies, which will be made available where applicable.

We will review and update this policy following our data protection obligations. It does not form part of any employee’s contract of employment, and we may amend, update, or supplement it from time to time.

We will circulate any new or modified policy to staff and any other stakeholders when it is adopted.

Definitions

Criminal Records Information	Means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
Data Subject	Means the individual to whom the personal information relates;
Personal Information	(Sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
Processing Information	Means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
Pseudonymised	Means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

Sensitive Personal Information	Sometimes known as 'special categories of personal data' or 'sensitive personal data' means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.
Processor	The UK GDPR defines a processor as: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.
Controller	Art.2(d) GDPR "Controller" means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws.

Data Protection Principles

the Michael Lonsdale Group will comply with the following data protection principles when processing personal information:

- We will process personal information lawfully, fairly and in a transparent manner;
- We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- We will only process the personal information that is adequate, relevant, and necessary for the relevant purposes;
- We will keep accurate and up-to-date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- We will keep personal information for no longer than is necessary and for the purposes for which the information was collected for processing; and
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

The Basis for Processing Personal Information

Concerning any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

- Review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing, for example:
    - That the data subject has consented to the processing;
    - That the processing is necessary for the performance of a contract to which the data subject is party;
    - To take steps at the request of the data subject before entering into a contract;
    - That the processing is necessary for compliance with a legal obligation to which the Michael Lonsdale Group is subject;

- That the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
- That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
    - That the processing is necessary for legitimate interests of the Michael Lonsdale Group or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the Data Subject.

- Except where the processing is based on consent, the Michael Lonsdale Group has satisfied **ourselves** that the processing is necessary for the relevant lawful basis (for example, that there is no other reasonable way to achieve that purpose).
- Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).
- Where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it; and
- Where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

- Determine whether the Michael Lonsdale Group's legitimate interests are the most appropriate basis for lawful processing, we will:
    - Conduct a Legitimate Interest's Assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
    - If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
    - Keep the LIA under review, and repeat it if circumstances change; and
    - Include information about our legitimate interests in our relevant privacy notice(s).

Sensitive Personal Information

Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

- the Michael Lonsdale Group may need to process sensitive personal information. We will only process sensitive personal information if:
    - We have a lawful basis for doing to set out above, for example, it is necessary for the performance of the employment contract, to comply with the Michael Lonsdale Group's legal obligations for people or for the Michael Lonsdale Group's legitimate interests; and
    - One of the special conditions for processing sensitive personal information applies, for example:
        - The data subject has given explicit consent so the Michael Lonsdale Group can provide its services.
        - The processing is necessary for exercising the employment law rights or obligations of the Michael Lonsdale Group or the data subject.
        - The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
        - Processing relates to personal data which are manifestly made public by the data subject.
        - The processing is necessary for the establishment, exercise, or defence of legal claims; or
        - The processing is necessary for reasons of substantial public interest.

- Before processing any sensitive personal information, staff must inform the DPO of the proposed processing, so that the data protection officer may assess whether the processing complies with the criteria noted above.

- Sensitive personal information will not be processed until:
    - The assessment/training has been agreed to; and

- The individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

- **the Michael Lonsdale Group will not carry out automated decision-making (including profiling) based on an individual's sensitive personal information.**

- the Michael Lonsdale Group's **Privacy Notice** sets out the types of sensitive personal information that the Michael Lonsdale Group processes, what it is used for and the lawful basis for the processing.

- Concerning sensitive personal information, the Michael Lonsdale Group will comply with the procedures set out to make sure that it complies with the data protection principles set out above.

- During the recruitment process: the company will ensure that (except where the law permits otherwise):

  - During the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, for example, race or ethnic origin, trade union membership or health;

  - If sensitive personal information is received, for example, the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

  - Any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing, or making the recruitment decision;

  - '**Right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview, or decision-making stages;**

  - We will not ask health questions in connection with recruitment.

- During employment: the company will process:

  - Health information to administer sick pay, keeping sickness absence records, monitoring staff attendance, and facilitating employment-

related health and sickness benefits;

- Sensitive personal information for equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised; and

Criminal Records Information - Staff

Criminal records information will be processed following the Michael Lonsdale Group requirements for DBS (Disclosure and Barring Service) checks on a case-by-case basis.

Data Protection Impact Assessments (DPIAs)

Where the processing is likely to result in a high risk to an individual's data protection rights, either for internal the Michael Lonsdale Group business operations or the execution of a client contract, we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate concerning its purpose.
- The risks to individuals; and
- What measures can be put in place to address those risks and protect personal information.
- Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer so that a DPIA can be carried out.
- During any DPIA, the **appropriate officer within the Michael Lonsdale Group** will seek the advice of the data protection officer and any other relevant stakeholders.

Documentation and Records

We will keep records of processing activities, including:

- The name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);
- The purposes of the processing;
- A description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Where possible, retention schedules; and
- Where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- Information required for privacy notices.
- Records of consent.
- Controller-processor contracts.
- The location of personal information.
- DPIAs; and
- Records of data breaches.
- If we process sensitive personal information or criminal records information, we will keep written records of:
    - The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
    - The lawful basis for our processing; and

  - Whether we retain and erase the personal information following our policy document and, if not, the reasons for not following our policy.

- We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:
  - Carrying out information audits to find out what personal information the Michael Lonsdale Group holds.
  - Distributing questionnaires and talking to staff across the Michael Lonsdale Group to get a more complete picture of our processing activities; and
  - Reviewing our policies, procedures, contracts, and agreements to address areas such as retention, security, and data sharing.
- We document our processing activities in electronic form so we can add, remove, and amend information easily.

General Controls in Place

- There is a process of continual review to determine whether any changes in the organisation's registration are required as a result of changes in the nature of the business.
- The details of the Michael Lonsdale Group are registered are kept up to date.
- The notification to the Information Commissioner's Office is renewed annually.
- the Michael Lonsdale Group maintains and updates the public data protection register which will be reviewed regularly and at least on an annual basis.

Privacy Notices

The Michael Lonsdale Group will issue privacy notices from time to time, informing individuals about the personal information that we collect and hold relating to them, how they can expect their personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

Individual Rights

Individuals have the following rights concerning their personal information:

- To be informed about how, why and on what basis that information is processed.
- To obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a Subject Access Request (SAR") – please see the SAR Policy information.
- To have data corrected if it is inaccurate or incomplete;
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten);
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim; and
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).
- If you wish to exercise any of the rights in the paragraphs above, please contact the data protection officer.

Individual Obligations

Individuals are responsible for helping the Michael Lonsdale Group keep their personal information up to date. You should let the Michael Lonsdale Group know if the information you have provided to the Michael Lonsdale Group changes, for example, if you move to a new house or change details of the bank or building society account to which you are paid.

You may have access to the personal information of other members of staff, suppliers, and clients of the Michael Lonsdale Group in the course of your employment or engagement. If so, the Michael Lonsdale Group expects you to help meet its data protection obligations to those

individuals. For example, you should be aware that they may also enjoy the rights set out above.

If you have access to personal information, you must:

- Only access the personal information that you have authority to access, and only for authorised purposes;
- Only allow other staff to access personal information if they have appropriate authorisation;
- Only allow individuals who are not the Michael Lonsdale Group staff to access personal information if you have specific authority to do so from the data protection officer.
- Keep personal information secure (for example. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Michael Lonsdale Group's IT Security Policy).
- Not remove personal information, or devices containing personal information (or which can be used to access it), from the Michael Lonsdale Group's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- Not store personal information on local drives or on personal devices that are used for work purposes.
- You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or is likely to take place):
    - Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions being met;
    - Any data breach as set out below;
    - Access to personal information without the proper authorisation;

- Personal information not kept or deleted securely;
- Removal of personal information, or devices containing personal information (or which can be used to access it), from the Michael Lonsdale Group's premises
  without appropriate security measures being in place;
- Any other breach of this Policy, or any of the data protection principles set out above.

Information Security

The Michael Lonsdale Group will use appropriate technical and organisational measures to keep personal information secure and to protect against unauthorised or unlawful processing and accidental loss, destruction, or damage. These may include:

- Making sure that, where possible, personal information is pseudonymised or encrypted;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored promptly; and
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- In rare cases where the Michael Lonsdale Group uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:
  - The organisation may act only on the written instructions of the Michael Lonsdale Group;

- Those processing the data are subject to a duty of confidence;
- Appropriate measures are taken to ensure the security of processing;
- Sub-contractors are only engaged with the prior consent of the Michael Lonsdale Group and under a written contract.
- The organisation will assist the Michael Lonsdale Group in providing subject access and allowing individuals to exercise their rights under the GDPR;
- The organisation will assist the Michael Lonsdale Group in meeting its GDPR obligations concerning the security of processing, the notification of data breaches and data protection impact assessments;
- The organisation will delete or return all personal information to the Michael Lonsdale Group as requested at the end of the contract; and
- The Michael Lonsdale Group will submit to audits and inspections, provide the Michael Lonsdale Group with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Michael Lonsdale Group immediately if it is asked to do something infringing data protection law.

- Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer.

Storage and Retention of Personal Information

- Personal information (and sensitive personal information) will be kept securely following the Michael Lonsdale Group's Data Security Policy.
- Personal information (and sensitive personal information) should not be retained any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the Michael Lonsdale Group's retention periods which set out the relevant period or the criteria that should be used to determine the retention period. Where there is any

uncertainty, staff should consult the data protection officer

- Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data Breaches

- A data breach may take many different forms, for example:
    - Loss or theft of data or equipment on which personal information is stored;
    - Unauthorised access to or use of personal information either by a member of staff or third-party;
    - Loss of data resulting from an equipment or systems (including hardware and software) failure;
    - Human error, such as accidental deletion or alteration of data;
    - Unforeseen circumstances, such as a fire or flood;
    - Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
    - 'Blagging' offences, where information is obtained by deceiving the organisation which holds it.
- In the event of a Data Breach, the Michael Lonsdale Group will:
    - Make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals;
    - Notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.
    - Risk assesses the situation and determine what steps need to be taken.
    - Immediately take such steps as are necessary to minimise the risk to clients, staff, and the organisation.
    - Take such steps as are necessary to ensure that similar breaches cannot happen again.

Please refer to our **Incident Management Policy** for more information.

International Transfer of Data

The Michael Lonsdale Group does not intend to transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to other countries.

If this were to be required, it would be on the basis that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses.

Consequences of Failing to Comply

The Michael Lonsdale Group takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and the Michael Lonsdale Group; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, a staff member's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer.

Client/Persons Data Storage and Retention

The Michael Lonsdale Group provides clients with a full range of mechanical, electrical and public health services.

We store a limited amount of clients information to manage their projects and accounts.

Systems Used and Data Stored – Clients

The following core systems are used to store clients data defined in Clients Data Stored.

Access is only provisioned to the staff members who work with the clients and software access controls are managed internally.

Please refer to the Michael Lonsdale Group **Access Controls Policy** for more information on the Principle of Least Privilege.

The systems typically used are:

- Microsoft 365 productivity tools including PowerPoint, Excel, and Word.
- Microsoft SharePoint and Teams.
- On premise legacy shared folders (being phased out).
- Autodesk AEC Collection – CAD Modelling & Drafting.
- Autodesk Build – Snagging and Commissioning.
- Elecosoft Power Project – Production of Project Programmes.

Systems Used and Data Stored – Staff

SharePoint is primarily used to store information – with the data residing in secure folders.

Other Systems used may contain limited amounts of data.:

- RedSky Summit Financial Software.
- Induction information is stored in locked files onsite (being phased out).

Sharing of Data – Clients/Staff

Staff and client data is only shared when required with the following individuals and organisations:

- HMRC.
- Welfare organisations (if required).
- Police and Government related organisations (if required).

All accounting and HR functions are managed in-house.

Clients Data Stored

This table details the specific data types stored for Client Business or Personal Data, the reason the data is processed, along with the legal/legitimate reason as well as the expected retention period.

Information Type
Client Business Data
Data Stored
• Client contact details (Name, Address, Phone Numbers, Email). • Client-specific project information including quotes, proposals and project data.
Processing Reason
• Administration and Management of the Michael Lonsdale Group services. • Marketing of the Michael Lonsdale Group services.

Legal Interest/Legitimate Reason
• Legitimate reason for performing contract duties. • Consent is given by an individual representing the client at a contract or opt-in stage.
Retention Policy
12 years from project termination.

Staff Data Stored

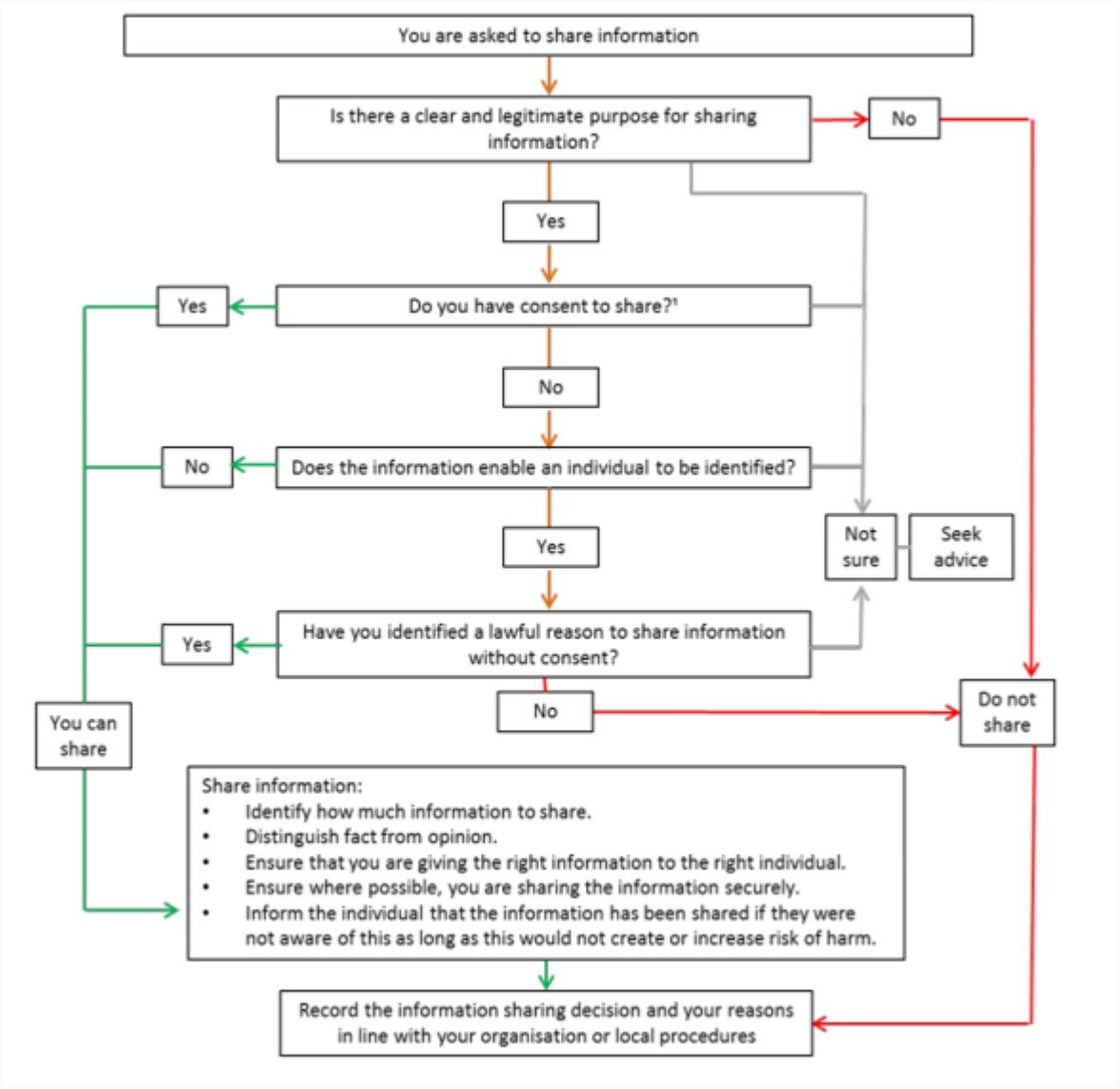
This table details the specific data types stored for the Michael Lonsdale Group Staff, the reason the data is processed, along with the legal/legitimate reason as well as the expected retention period.

Information Type
Staff Data
Data Stored
Typical staff information stored: **Personal Information** • Name, address, email, telephone number. • Next of Kin. • Application Form data/CV. • Interview notes. • Offer and acceptance letters **Contract** • Dated/signed. • P60/P45. **Photographic Evidence of Identity** • Valid Passport/Driving Licence copy. **Various** • National Insurance/UTR and Bank details. • Copies of relevant qualifications. • Right to Work in the UK

• Evidence of Current Address • References. • Training Record. • Record of sickness, leave and disciplinaries. • Statutory Maternity, Adoption, Paternity Pay • Statutory Sick Pay • Payroll and PAYE Records • Health and Safety Consultations • Redundancy Details • Disciplinary, working time and training data For subcontractors, basic payment data (invoicing company, for example) is stored only along with selected required information from above.
Processing Reason
• Provision of employment obligations. • Fulfilment of contract.
Legal Interest/Legitimate Reason
• Legitimate reason for performing contract duties. • Consent is given by an individual at the initial stage (contract).
Retention Policy
6 years after the end of employment. 40 years for liabilitised health issues, such as Asbestos,

Data Sharing Process Flow – Clients

The below diagram represents a typical process flow for UK GDPR data sharing, the controls around data sharing and the actions that should be taken before sharing data.



Subject Access Requests and Data Rights – Clients and Staff

Introduction

Under GDPR legislation, Data Controllers shall provide the information outlined in Articles 13 & 14 to Data Subjects and Data Subjects may access, correct, delete, restrict processing of, and transfer their personal data, as well as to object to automated decision-making based on their personal data.

SAR and Data Rights Procedure

Subject Access Requests should come to the DPO email address in the first instance and be followed up with an acknowledgement letter/email.

All requests and their progress must be logged by the data protection officer in a secure place with no external access.

SAR Timescales

All Subject Access Requests will be completed within 30 days unless defined as complex.

If the time will exceed 30 days, the requestor will be notified by return email to their request submitted to the DPA email address Jonathan.Wallace@michaellonsdale.com

SAR Fee's

Subject Access Requests coming directly from the data subject will be free, however, the Michael Lonsdale Group can charge a fee if requests become unfounded or excessive. If requests are coming from a client on behalf of a data subject, the Michael Lonsdale Group may charge a fee for data retrieval.

SAR Business Processes

The processes cover SAR and other data rights of individuals:

- Right of Access and Data Portability
- Right to Erasure
- Right to Object
- Right to Restriction
- Right to Rectification

Undertaking Privacy Impact Assessments

When the Michael Lonsdale Group undertakes the use of new technologies or will be involved in the processing of data that contains a high risk to the rights and freedoms of data subjects, it will undertake a Privacy Impact Assessment.

The scale and nature of each PIA will be shaped on a case-by-case basis to capture the following information to inform the decision-making process:

- Risk Assessment
- Data types, collection, storage use and deletion methodologies
- Legal basis
- Information flows processes and procedures
- Consultation
- Evaluation of privacy procedures
- Final summary

For further information on PIA Please refer to:

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Confidentiality

We do not disclose information given to us to third parties without consent, unless required under our safeguarding policies and procedure or our obligations to the Data Protection Act 1998 and GDPR 2019/UK GDPR 2021.

All breaches will be taken seriously and are potentially a disciplinary matter.

There are, however, exemptions for breaches of confidentiality under special circumstances.

Any actual or suspected breaches of Confidentiality shall be reported at once to a the Michael Lonsdale Group director who will immediately:

- Risk assesses the situation and determine what steps need to be taken.
- Immediately take such steps as are necessary to minimise the risk to clients, staff and the business.
- Take such steps as are necessary to ensure that similar breaches cannot happen again.

Clients

It is necessary to collect and keep a certain amount of information about our clients, however:

- We only collect and keep information that is necessary to enable us to perform our services.
- Access to the information held on people is restricted to the Michael Lonsdale Group staff.
- Information is not made available to third parties without the informed specific consent of the person (or by exceptions under the Data Protection Act 1998/UK GDPR).
- When collecting information, we should always inform them why information is required and what it will be used for.
- Subcontractors working for the Michael Lonsdale Group are also required to comply with our confidentiality policy.

Discussions and Meetings

- If discussing a person's situation in a meeting, staff should only disclose information relevant to the matter at hand.
- Staff should be aware that others with no involvement may be able to overhear e.g., at reception, in an open-plan office or corridors. Staff will ensure discussions happen in an appropriate place.
- Staff will not discuss personal facts about one person or company with or in the presence of, any other person.

Outside of Work

- Staff should regard all information they have access to or are given as a result of their work for the Michael Lonsdale Group as being confidential at all times unless advised otherwise.
- When working remotely, all personal and sensitive information should be kept in locked storage and should only be shared through secured systems, i.e., using password-protected documents, secure platforms, etc.

Requests for Information

- People have a right to request access to information kept about them. The request must be put in writing and dealt with by the appropriate director.
- Third parties may request information about a person. This should only be given if we have received formal consent from the person. There may be certain exceptions - See Data Protection and Safeguarding policies.
- The release of this confidential information must be determined by a company director.

Access to Records

Under GDPR legislation, Data Controllers shall provide the information outlined in Articles 13 & 14 to Data Subjects and Data Subjects may access, correct, delete, restrict processing of, and transfer their data, as well as to object to automated decision-making based on their data.

- GDPR gives persons the right to access the personal data held about them by the Michael Lonsdale Group through Subject Access Requests, specifically persons have the following rights:
    - Right of Access and Data Portability
    - Right to Erasure
    - Right to Object
    - Right to Restriction
    - Right to Rectification

- All Subject Access Requests will be completed within 30 days unless defined as complex – if the time will exceed 30 days, the requestor will be notified.

- Information requested by a person may cover both manual and computerised records. These requests should be processed in the same way as requests to view paper records.

- Subject Access Requests coming directly from the data subject will be free, however, the Michael Lonsdale Group can charge a fee if requests become unfounded or excessive.

Security of Personal Data

the Michael Lonsdale Group will ensure that personal data is held securely and for no longer than is necessary.

If you believe you have lost any personal data in the course of your work, you must report it immediately.

Failure to do so may result in disciplinary action up to and including dismissal.

Disclosure Policy

the Michael Lonsdale Group will not allow personal and sensitive personal data collected from persons to be disclosed to third parties except in circumstances that meet the requirements of our defined legal basis or other controls defined by GPDR.

Example situations are when:

- The person has consented to the disclosure.
- There is a serious risk of harm.
- Where the Michael Lonsdale Group receives information that may prevent a crime or assist in the detection of a crime.
- Where the Michael Lonsdale Group is legally obliged to disclose the data.

Procedure on Disclosures

Any disclosure to be made must be checked for suitability beforehand and the individual performing the check may refer to the Information Commissioner for advice and guidance.

Any request for data based on a legal requirement, e.g., from the Police or other body, must be put in writing and be checked by a director or the DPO against the advice of the Information Commissioner before any data is disclosed.

Staff Records

It is necessary to collect and keep a certain amount of information about current, former, and potential staff.

Our confidentiality policy aims to safeguard privacy and ensure appropriate access to information:

- The processing of all information is governed by GDPR 2018.
- We only collect and keep the necessary information to perform roles and manage HR and payroll administration.
- Access to information collected is restricted to the Human Resources staff, the staff members and company directors.
- Information is not made available to third parties without the informed consent of the staff member (or exceptions as in the Data Protection Policy or exceptions under the safeguarding policies and procedures).
- When collecting information from a staff member we should always inform them why information is required and what it will be used e.g., for supervision purposes.
- Personal facts about one staff member are not discussed with, or in the presence of, any other person
- Staff will not disclose personal details (home address, telephone number etc.) to persons or other parties but should use their project address when an address must be given.

Outside of Work

Staff must adhere to the Confidentiality and Data Protection policies and procedures at all times.

Personal and Sensitive Information

the Michael Lonsdale Group will process sensitive data such as medical information and DBS checks, primarily where it is necessary to enable the Michael Lonsdale Group to meet its legal obligations and in particular to ensure adherence to health and safety and vulnerable groups protection legislation or for equal opportunities monitoring purposes.

the Michael Lonsdale Group will not process sensitive personal data without consent.

Requests for Information

Staff have the same Subject Access Requests rights as clients.

Disclosure Policy and Procedures

The Michael Lonsdale Group will not allow personal and sensitive personal data collected from employees to be disclosed to third parties except in circumstances that meet the requirements of GDPR 2018/UK GDPR 2021.

This will be where either the employee has consented to the disclosure, or there is a serious risk of harm and where the Michael Lonsdale Group receives information that may prevent a crime or assist in the detection of a crime, or where the Michael Lonsdale Group is legally obliged to disclose the data.

Procedure on Disclosures

Any disclosure to be made must be checked for suitability with a company director who may refer to the Information Commissioner for advice and guidance.

Any request for data based on a legal requirement, e.g., from the Police or other body, must be put in writing and be checked by a company director against the advice of the Information Commissioner before any data is disclosed.

Name: Gary Herbert For and on behalf of the MLG Board of Directors

Position: Chief Executive Officer

Signature: 

Date 10/01/2023