MMC Privacy Policy

1. Introduction

This Privacy Policy sets out how MMC handles the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

It applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for us to comply with the current law. Your compliance is mandatory. And any breach of this Policy may result in disciplinary action up to and including dismissal with or without notice.

This is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from Marsha Cox.

2. Employee rights and choices

Your personal data is held for the specific purposes of:

- Achieving a legitimate business aim and/or management of vital interests.
- Compliance with regulatory legislative requirements
- Administration of contractual employment agreements

Outside of these interests any other use of your personal data including your personal image will require your explicit consent.

The Data Protection Act (GDPR) 2018 provides Employees with the following rights:

• The right to be informed • The right of access

• The right of rectification • The right of erasure

• The right to restrict processing

• The right to data portability

• The right to object

• The right not to be subject to automated decision-making including profiling

• The right to submit subject access requests

You should consult our Privacy Policy for further information on how your data is stored and for long it is retained.

Should you wish to make a Data Subject Request to review the personal information held by the Consultancy, please make your request in writing, to Marsha Cox.

3. Scope

The correct and lawful treatment of Personal Data and protection of the confidentiality and integrity of Personal Data is a critical responsibility that must be taken seriously at all times.

The Business is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

Marsha Cox is responsible for overseeing this Policy. Please contact them with any questions about the operation of the Policy or if you have any concerns that this Policy is not being or has not been followed.

In particular, you must always contact Marsha Cox in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Business)

(b) if you need to rely on Consent and/or need to capture Explicit Consent

(c) if you need to draft Privacy Notices

(d) if you are unsure about the retention period for the Personal Data being Processed

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data

(f) if there has been a Personal Data Breach

(g) if you are unsure on what basis to transfer Personal Data outside the EEA

(h) if you need any assistance dealing with any rights invoked by a Data Subject

(i) whenever you are engaging in a significant new, or change in, Processing activity or plan to use Personal Data for purposes others than what it was collected for;

(j) If you need help complying with applicable law when carrying out direct marketing activities; or

(k) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our suppliers).

4. Personal Data Protection Principles

The following principles relating to Processing of Personal Data set out in the Data Protection Act (GDPR) 2018 must be followed.

Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

- Lawfulness, Fairness, Transparency

We may only collect, Process and share Personal Data fairly and lawfully and for specified purposes.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Processing is necessary for the performance of a contract with the Data Subject.

(b) to meet our legal compliance obligations.

(c) the Data Subject has given his or her Consent.

(d) to protect the Data Subject's vital interests.

(e) to pursue our legitimate interests for purposes where they do not override the interests or fundamental rights and freedoms of Data Subjects.

You must identify and document the legal ground being relied on for each Processing activity. For all grounds, evidence must be obtained and retained.

a) Consent

The Company as a Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject must positively OPT IN to consent to Processing of their Personal Data. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.

Consent must be easy to withdraw and withdrawal must be promptly honoured. We may need to refresh consent where the data will be used for a different reason.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually, we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, please contact Marsha Cox.

- Transparency (notifying data subjects)
  - In accordance with the GDPR, we will provide Privacy Notices to all Data Subjects, through correspondence, terms of business and our website.
  - Privacy Notices will provide all the information required by the GDPR including, how and why we will use, Process, disclose, protect and retain that Personal Data. Privacy notices must be presented when the Data Subject first provides the Personal Data.

5. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

6. Data Minimisation

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Business data retention guidelines.

7. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

8. Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Business will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. All data on employees must be retained with Marsha Cox.

9. Security Integrity and Confidentiality

- Protecting Personal Data:
    - Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. The Business has put systems in place and will continue to develop those systems in compliance with GDPR.
    - You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.
    - You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers with written confirmation and consent from Marsha Cox.
    - You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

        (a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

        (b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

        (c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

- Reporting a Personal Data Breach:
  - Any Personal Data Breach MUST be notified to the applicable regulator and, in certain instances, the Data Subject.
  - Any such breaches will be deal with by Marsha Cox. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact Marsha Cox. You should preserve all evidence relating to the potential Personal Data Breach.

10. Transfer Limitation

You must not transfer any data outside of the EEA without authorisation from Marsha Cox.

11. Data Subject's Rights and Requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time.

(b) receive certain information about the Data Controller's Processing activities.

(c) request access to their Personal Data that we hold.

(d) prevent our use of their Personal Data for direct marketing purposes.

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.

(f) restrict Processing in specific circumstances.

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest.

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA.

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else.

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms.

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must immediately forward any Data Subject request you receive to your supervisor and Marsha Cox.

12. Accountability

- As the Data Controller, we must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.
- Record keeping:
  - The GDPR requires us to keep full and accurate records of all our data Processing activities.
  - You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents
- Training and audit:
  - We are required to ensure all Company Personnel have adequate training to enable them to comply with data privacy laws. We must also test our systems and processes to assess compliance.
  - You must comply with all data privacy related training.
  - You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.
- Direct marketing:
  - We are subject to certain rules and privacy laws when marketing to our clients.
  - For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing clients known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.
  - The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. A Data Subject's objection to direct marketing must be promptly honoured.

13. Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services.

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained.

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

You must comply with the Company's guidelines on sharing data with third parties.

Definitions:

Company/Business name: MMC

Company Personnel: all employees, workers contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

14. Monitoring and Review

MMC will monitor the effectiveness of this policy and its procedures. This policy will be reviewed annually and updated as necessary to ensure compliance with legislation and best practices. Employees will be informed of any changes to this policy.

15. Contact Information

For any questions or concerns regarding this policy, please contact:

MMC:

2 – 4 East Street, Newton Abbot, Devon TQ12 1AF

Mrs Marsha Cox marsha@mmcltd.co.uk

16. Policy Approval

This Policy has been approved by Marsha Cox. Any amendments or updates will be communicated to all employees.

Signed: 

[Name] Marsha Cox

[Title] Managing Director

[Date] 15th December 2025