Date Protection Policy

1. POLICY STATEMENT AND SCOPE OF POLICY

1.1

Monoworld Group ("the Company", "we", "our" or "us") is committed to protecting the privacy, confidentiality, integrity and security of personal data processed as part of its business activities.

The Company will ensure that personal data is processed lawfully, fairly and transparently and in accordance with applicable data protection legislation.

1.2

The Company recognises that individuals have rights in relation to the processing of their personal data. During the course of its activities, the Company may collect, receive, store, use, disclose and otherwise process personal data relating to employees, workers, officers, consultants, customers, suppliers, contractors, job applicants, visitors and other individuals.

The Company is committed to ensuring that all personal data is handled appropriately, securely and lawfully.

1.3

Employees, workers, officers, consultants, agency workers and other persons working for or on behalf of the Company have responsibilities when processing personal data.

All such persons are required to comply with this Policy and with any associated procedures, instructions and information-security requirements issued by the Company.

1.4

This Policy sets out how the Company will handle personal data relating to:

- **Customers;**
- **Suppliers;**
- **Employees and workers;**
- **Officers and directors;**
- **Consultants and contractors;**
- **Agency workers;**
- **Job applicants;**
- **Work placement students;**
- **Visitors;**
- **Business contacts and prospects;**
- **Service providers; and**
- **Other third parties whose personal data is processed by the Company.**

The Policy establishes the Company's requirements for the lawful, fair, secure and responsible processing of personal data.

1.5

In this Policy, “you” or “your” refers to employees, workers, officers, consultants, agency workers and other individuals engaged by or working on behalf of the Company.

1.6

This Policy is intended to ensure compliance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Data (Use and Access) Act 2025, where applicable, and any other legislation, regulatory requirements or guidance governing the processing of personal data.

These are collectively referred to in this Policy as the “Data Protection Laws”.

1.7

This Policy does not form part of an employee's contract of employment and the Company reserves the right to amend it where necessary.

Any breach of this Policy will be taken seriously and may result in disciplinary action in relation to employees or other appropriate action in relation to non-employees.

Serious breaches may constitute gross misconduct and may result in dismissal or termination of an individual's engagement, where appropriate.

---

2. DEFINITION OF DATA PROTECTION TERMS USED IN THIS POLICY

2.1 Automated Decision-Making

Automated Decision-Making (ADM) means a decision made by automated means without meaningful human involvement.

Where automated processing is used to make a decision that has a legal or similarly significant effect on an individual, the Company will ensure that the processing complies with applicable Data Protection Laws and that appropriate safeguards are implemented.

2.2 Automated Processing

Automated processing means processing personal data using automated means.

This may include the use of software, algorithms or systems to analyse or evaluate information relating to an individual.

Profiling is a form of automated processing.

2.3 Consent

Consent means a freely given, specific, informed and unambiguous indication of an individual's wishes by which they signify agreement to the processing of their personal data.

Where consent is required to process special category personal data, the consent must meet the applicable requirements for explicit consent.

2.4 Criminal Offence Data

Criminal offence data means personal data relating to criminal convictions and offences or related security measures.

Such information will only be processed where permitted by applicable Data Protection Laws and where an appropriate lawful basis and condition applies.

2.5 Data

Data includes information stored electronically, on computers, servers, databases or other electronic systems, as well as certain paper-based filing systems.

2.6 Data Controller

A Data Controller is the person or organisation that determines the purposes and means of processing personal data.

The Company acts as Data Controller for personal data processed for its own business purposes, including information relating to employees, workers, officers, consultants, job applicants, customers, suppliers, visitors and business contacts.

2.7 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process used to identify, assess and mitigate data protection risks associated with processing activities, particularly where processing is likely to result in a high risk to individuals.

2.8 Data Subjects

A Data Subject is an identified or identifiable living individual to whom personal data relates.

A Data Subject does not need to be a UK national or resident.

2.9 Explicit Consent

Explicit consent is consent given through a clear and specific statement or other clear affirmative action where the circumstances require a higher standard of consent.

2.10 Personal Data

Personal data means information relating to an identified or identifiable living individual.

An individual may be identifiable directly or indirectly through information held by the Company or reasonably available to it.

Personal data may include, for example:

- **Names;**
- **Addresses;**
- **Telephone numbers;**
- **Email addresses;**
- **Employee information;**

- **Identification information;**
- **CCTV images;**
- **Vehicle registration information;**
- **Financial information;**
- **Employment records; and**
- **Online identifiers.**

Personal data does not include genuinely anonymous information where an individual can no longer be identified.

2.11 Personal Data Breach

A Personal Data Breach means a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples include:

- **Sending personal information to the wrong recipient;**
- **Loss or theft of equipment containing personal data;**
- **Unauthorised access to systems;**
- **Accidental disclosure of personal information;**
- **Cyber attacks;**
- **Malware or ransomware incidents;**
- **Loss of paper records; or**
- **Unauthorised alteration or destruction of personal data.**

2.12 Privacy Notices

Privacy Notices are documents that provide individuals with information about how their personal data is collected, used, stored and shared.

Privacy Notices will include information required by applicable Data Protection Laws.

2.13 Processing

Processing means any operation performed on personal data, whether by automated means or otherwise.

Processing includes:

- **Collection;**
- **Recording;**
- **Organisation;**
- **Storage;**
- **Retrieval;**

- **Consultation;**
- **Use;**
- **Disclosure;**
- **Transmission;**
- **Restriction;**
- **Amendment;**
- **Erasure; and**
- **Destruction.**

2.14 Pseudonymisation

Pseudonymisation means processing personal data so that it can no longer be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and appropriately protected.

2.15 Special Category Personal Data

Special category personal data is personal data requiring additional protection because it is particularly sensitive.

This may include information relating to:

- **Racial or ethnic origin;**
- **Political opinions;**
- **Religious or philosophical beliefs;**
- **Trade union membership;**
- **Genetic data;**
- **Biometric data where used for identification;**
- **Health;**
- **Sex life; and**
- **Sexual orientation.**

Special category personal data will only be processed where the Company has an appropriate lawful basis and an applicable additional condition under Data Protection Laws.

---

3. DATA PROTECTION RESPONSIBILITIES

3.1

The Company is responsible for ensuring that appropriate arrangements are in place to comply with applicable Data Protection Laws and this Policy.

3.2

Overall responsibility for data protection compliance rests with the Company's senior management.

The Compliance Director and relevant members of management will oversee data protection matters as appropriate to their responsibilities.

3.3

Managers and supervisors are responsible for ensuring that employees and workers within their areas of responsibility understand and comply with this Policy.

This includes ensuring that:

- **Personal data is only accessed where there is a legitimate business need;**
- **Appropriate security measures are followed;**
- **Data protection concerns are escalated appropriately;**
- **Personal data breaches are reported without delay;**
- **Appropriate retention requirements are followed; and**
- **Employees receive any required training.**

3.4

Employees, workers, officers, consultants and other persons working for or on behalf of the Company are responsible for ensuring that they:

- **Process personal data only for legitimate and authorised purposes;**
- **Keep personal data confidential;**
- **Follow Company procedures and instructions;**
- **Protect personal data against loss or unauthorised disclosure;**
- **Only access information necessary for their role;**
- **Report actual or suspected data breaches immediately; and**
- **Complete required data protection training.**

3.5

Where specialist advice is required, the Company may obtain advice from appropriately qualified external advisers or other competent persons.

3.6

Where the Company is legally required to appoint a Data Protection Officer, the Company will ensure that an appropriate individual is appointed and that the statutory requirements applicable to that role are met.

---

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1

The Company will comply with the data protection principles applicable under Data Protection Laws.

Personal data must be:

4.1.1 Lawfulness, Fairness and Transparency

Processed lawfully, fairly and transparently.

4.1.2 Purpose Limitation

Collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.

4.1.3 Data Minimisation

Adequate, relevant and limited to what is necessary for the purpose for which it is processed.

4.1.4 Accuracy

Accurate and, where necessary, kept up to date.

4.1.5 Storage Limitation

Not retained in an identifiable form for longer than is necessary for the purposes for which it is processed, subject to legal and regulatory retention requirements.

4.1.6 Integrity and Confidentiality

Processed securely using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.1.7 Accountability

The Company will be responsible for, and be able to demonstrate, compliance with these principles.

---

5. LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1

The Company will only collect, process and share personal data where there is a lawful basis for doing so and the processing is fair and transparent.

5.2

Depending on the circumstances, the Company may rely on one or more of the following lawful bases:

- **Consent;**
- **Contract;**
- **Legal obligation;**
- **Vital interests;**
- **Public task, where applicable; or**

- **Legitimate interests.**

The Company will identify and document the appropriate lawful basis for its processing activities.

5.3

Where the Company processes Special Category Personal Data, it must identify both:

1. **An appropriate lawful basis for processing; and**
2. **An applicable additional condition for processing special category data.**

These may include, where applicable:

- **Explicit consent;**
- **Employment and social protection obligations;**
- **Protection of vital interests;**
- **Information made public by the Data Subject;**
- **Establishment, exercise or defence of legal claims;**
- **Occupational health;**
- **Assessment of working capacity;**
- **Substantial public interest; or**
- **Other lawful conditions permitted by Data Protection Laws.**

5.4

Additional safeguards will be applied when processing Special Category Personal Data.

Access will be restricted to authorised personnel who have a legitimate business need to access the information.

---

6. CONSENT

6.1 Employees, Workers, Officers and Consultants

6.1.1

The Company will only rely on consent where it is an appropriate lawful basis.

In employment situations, consent will generally not be relied upon where another lawful basis is more appropriate.

6.1.2

Where consent is requested, it must be freely given, specific, informed and unambiguous.

6.1.3

Where the Company relies on consent, the individual will be informed that consent may be withdrawn and will be provided with a clear method for doing so.

6.1.4

The Company will maintain appropriate records of consent where consent is relied upon as the lawful basis for processing.

6.2 Customers, Contacts, Suppliers and Business Prospects

6.2.1

The Company may process personal data relating to customers, suppliers, business contacts and prospects where it has a lawful basis to do so.

This may include processing for:

- **Contract administration;**
- **Account management;**
- **Business communications;**
- **Marketing;**
- **Customer service;**
- **Supplier management;**
- **Business development; and**
- **Other legitimate business purposes.**

6.2.2

Where consent is legally required for marketing or other processing activities, the Company will obtain and manage that consent appropriately.

---

7. TRANSPARENCY – PRIVACY NOTICES

7.1

The Company will provide appropriate privacy information to Data Subjects when personal data is collected or when the purposes of processing materially change.

Privacy Notices will explain, where applicable:

- **What personal data is collected;**
- **How it is collected;**
- **Why it is processed;**
- **The lawful basis for processing;**
- **Any additional conditions relied upon for Special Category Personal Data;**
- **Who the information may be shared with;**

- **How long the information will be retained;**
- **The Data Subject's rights;**
- **How to raise a complaint; and**
- **Other information required by applicable Data Protection Laws.**

7.2

Privacy Notices will be reviewed periodically to ensure they remain accurate and reflect the Company's actual processing activities.

---

8. PURPOSE LIMITATION

8.1

Personal data will only be used for specified, explicit and legitimate purposes.

The Company will not use personal data for a new or incompatible purpose unless the proposed processing is lawful and appropriate under Data Protection Laws.

8.2

Where the purpose of processing changes, the Company will assess whether additional privacy information, a new lawful basis or other safeguards are required.

8.3

Employees, workers, officers and consultants who need to process personal data for a purpose that has not been authorised must consult their line manager or another authorised Company representative before doing so.

---

9. DATA MINIMISATION

9.1

The Company will ensure that personal data processed is adequate, relevant and limited to what is necessary for the relevant purpose.

9.2

Employees, workers, officers and consultants must only process personal data where it is necessary for their role and authorised business activities.

9.3

Excessive or irrelevant personal data must not be collected, copied, retained or shared.

9.4

Employees should consider whether anonymisation or pseudonymisation can be used where identification of individuals is not required.

9.5

When personal data is no longer required, it must be securely deleted, destroyed or anonymised in accordance with the Company's retention requirements.

---

10. ACCURACY

10.1

The Company will take reasonable steps to ensure that personal data is accurate, complete and, where necessary, kept up to date.

10.2

Where inaccurate or incomplete information is identified, reasonable steps will be taken to correct or update it.

10.3

Employees, workers, officers and consultants must notify their line manager or appropriate Company representative when they become aware that personal data is inaccurate or out of date.

---

11. STORAGE LIMITATION

11.1

The Company will not retain personal data in an identifiable form for longer than is necessary for the purposes for which it was collected or processed, unless a longer retention period is required or permitted by law.

11.2

The Company will maintain appropriate retention schedules and procedures for different categories of personal data.

11.3

Retention periods may take account of:

- **Legal requirements;**
- **Regulatory requirements;**
- **Contractual obligations;**
- **Accounting requirements;**
- **Employment requirements;**
- **Health and safety requirements;**
- **Insurance requirements;**
- **Potential claims or disputes; and**
- **Legitimate business requirements.**

11.4

Employees, workers, officers and consultants must comply with applicable retention schedules and must not retain personal data indefinitely without justification.

11.5

Personal data that is no longer required must be securely deleted, destroyed or anonymised.

---

12. SECURITY, INTEGRITY AND CONFIDENTIALITY

12.1

The Company will maintain appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, alteration or damage.

12.2

Security measures may include:

- **Confidential and appropriately managed passwords;**
- **Access controls;**
- **User permissions;**
- **Encryption where appropriate;**
- **Secure backups;**
- **Anti-virus and anti-malware protection;**
- **Firewalls;**
- **Network security;**
- **System monitoring;**
- **Vulnerability assessments;**
- **Secure servers;**
- **Physical security;**
- **Secure disposal of confidential information; and**
- **Appropriate staff training.**

12.3

The Company's IT systems may be monitored, tested and reviewed for legitimate security, operational, compliance and business purposes in accordance with applicable Company policies and Data Protection Laws.

12.4

Employees, workers, consultants and officers are responsible for protecting personal data that they access or handle.

They must:

- **Keep passwords confidential;**
- **Not share login credentials;**
- **Lock devices when unattended;**
- **Take care when sending information by email;**
- **Protect paper records from unauthorised access;**
- **Report lost or stolen equipment immediately;**
- **Follow Company IT and information-security requirements; and**
- **Report suspected security incidents without delay.**

12.5

Employees must not attempt to bypass or disable the Company's administrative, physical or technical security controls.

---

13. REPORTING A PERSONAL DATA BREACH

13.1

All actual or suspected Personal Data Breaches must be reported immediately and without undue delay to the individual's line manager, Compliance Director or another authorised Company representative.

Employees must not delay reporting an incident while attempting to establish whether it constitutes a Personal Data Breach.

13.2

The Company will assess each breach to determine:

- **The nature and scope of the breach;**
- **The personal data involved;**
- **The number and categories of individuals affected;**
- **The likely consequences for individuals;**
- **The likelihood and severity of risk;**
- **What containment measures are required;**
- **Whether the ICO must be notified; and**
- **Whether affected individuals must be informed.**

13.3

Where a Personal Data Breach is notifiable to the ICO, the Company will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Not every Personal Data Breach is required to be reported to the ICO. However, all breaches must be appropriately assessed and recorded.

13.4

When reporting a breach, employees should provide as much information as possible, including:

- **What happened;**
- **When the incident occurred;**
- **When it was discovered;**
- **The type of personal data involved;**
- **The individuals potentially affected;**
- **The approximate number of records affected;**
- **Who may have received or accessed the information;**
- **Any immediate action taken; and**
- **Any evidence relevant to the incident.**

13.5

The Compliance Director or another authorised member of senior management will coordinate the Company's response to a Personal Data Breach and any required regulatory notification.

13.6

Employees must not report a Personal Data Breach directly to the ICO unless specifically authorised to do so.

13.7

All employees must cooperate fully with any internal or external investigation into a Personal Data Breach.

13.8

Employees must not attempt to conceal, alter or destroy evidence relating to a suspected breach unless specifically instructed to do so.

13.9

All Personal Data Breaches must be recorded, including incidents that are ultimately assessed as low risk and not notifiable to the ICO.

---

14. INTERNATIONAL TRANSFERS

14.1

The Company will comply with applicable UK requirements when transferring personal data outside the United Kingdom or otherwise making personal data available to recipients in other countries.

14.2

Before making a restricted international transfer, the Company will determine whether:

- **The destination is covered by applicable UK adequacy regulations;**
- **Appropriate safeguards are in place;**
- **A valid transfer mechanism is available; or**
- **A permitted exception applies.**

14.3

Where appropriate safeguards are required, these may include the UK International Data Transfer Agreement (IDTA), UK Addendum, Binding Corporate Rules or another lawful mechanism recognised under applicable Data Protection Laws.

14.4

Employees must not arrange or make an international transfer of personal data without appropriate authorisation where the transfer is subject to UK international transfer requirements.

---

15. INDIVIDUAL RIGHTS

15.1

Data Subjects have rights in relation to their personal data, subject to applicable legal conditions and exemptions.

These rights may include:

- **The right to be informed;**
- **The right of access;**
- **The right to rectification;**
- **The right to erasure;**
- **The right to restriction of processing;**
- **The right to data portability;**
- **The right to object;**
- **Rights relating to direct marketing;**
- **Rights relating to automated decision-making and profiling; and**
- **The right to withdraw consent where consent is the lawful basis for processing.**

15.2

Requests relating to an individual's data protection rights must be referred promptly to an appropriate authorised Company representative.

15.3

Employees must not independently delete, amend, disclose or withhold personal data in response to an individual's request unless authorised to do so.

15.4

The Company will respond to valid Data Subject requests within the applicable statutory timescales.

15.5

Where an exemption or restriction applies, the Company will assess the request in accordance with applicable Data Protection Laws.

---

16. ACCOUNTABILITY

16.1

The Company will implement appropriate technical and organisational measures to demonstrate compliance with applicable Data Protection Laws.

16.2

The Company will maintain appropriate documentation to demonstrate compliance, which may include:

- **Privacy Notices;**
- **Records of Processing Activities;**
- **Data Protection Impact Assessments;**
- **Legitimate Interest Assessments;**
- **Data retention schedules;**
- **Data breach records;**
- **Training records;**
- **Data processor agreements;**
- **Data sharing arrangements; and**
- **Data protection policies and procedures.**

16.3

The Company will periodically review its data protection arrangements to identify and address risks.

---

17. RECORD KEEPING

17.1

The Company will maintain appropriate records of its processing activities where required by Data Protection Laws.

17.2

Records will be maintained in a manner that enables the Company to demonstrate compliance with its data protection obligations.

17.3

Relevant records will be reviewed and updated when there are significant changes to the Company's processing activities, systems, suppliers or organisational arrangements.

---

18. TRAINING

18.1

The Company will ensure that employees, workers, consultants and officers who process personal data receive appropriate data protection training.

18.2

Training will cover, where relevant:

- **Data protection principles;**
- **Confidentiality;**
- **Information security;**
- **Personal data breaches;**
- **Individual rights;**
- **Phishing and cyber security;**
- **Secure use of email;**
- **Handling personal information;**
- **Data retention; and**
- **Reporting requirements.**

18.3

Employees whose roles require specific data protection knowledge may be required to undertake additional or specialist training.

18.4

Mandatory training must be completed within the timeframe specified by the Company.

Failure to complete mandatory training without reasonable justification may be dealt with under the Company's disciplinary procedures.

---

19. AUTOMATED PROCESSING AND AUTOMATED DECISION-MAKING

19.1

The Company may use automated processing and profiling where there is a lawful basis for doing so and the processing complies with applicable Data Protection Laws.

19.2

Where the Company proposes to use solely automated decision-making that has a legal or similarly significant effect on an individual, the processing must be assessed before implementation.

19.3

Where applicable, the Company will:

- **Provide individuals with appropriate information about the processing;**
- **Identify the lawful basis for the processing;**
- **Carry out a Data Protection Impact Assessment where required;**
- **Implement appropriate safeguards;**
- **Provide a means for individuals to challenge relevant decisions;**
- **Provide human intervention where legally required;**
- **Take steps to minimise errors and unfair outcomes; and**
- **Review the operation of the system periodically.**

19.4

Special care will be taken where Special Category Personal Data is involved in automated decision-making.

19.5

The Company will not introduce automated decision-making processes that have significant effects on individuals without appropriate legal, privacy and risk assessment.

---

20. SHARING PERSONAL DATA

20.1

The Company will only share personal data with third parties where there is a lawful basis and appropriate safeguards are in place.

20.2

Personal data may be shared with third-party service providers where necessary for legitimate business purposes, including:

- **Payroll providers;**
- **Pension providers;**
- **HR service providers;**
- **IT service providers;**

- **Recruitment agencies;**
- **Professional advisers;**
- **Insurers;**
- **Legal advisers;**
- **Contractors;**
- **Government departments;**
- **Regulatory authorities; and**
- **Other authorised service providers.**

20.3

Before sharing personal data with a third party, the Company will consider:

- **Whether the third party needs the information;**
- **Whether the disclosure is consistent with the relevant Privacy Notice;**
- **Whether there is an appropriate lawful basis;**
- **Whether the third party provides appropriate security measures;**
- **Whether a written contract is required;**
- **Whether the third party is acting as a Data Processor;**
- **Whether any international transfer requirements apply; and**
- **Whether the amount of information shared is limited to what is necessary.**

20.4

Where a third party acts as a Data Processor on behalf of the Company, an appropriate written agreement will be put in place where required by Data Protection Laws.

20.5

The Company will take reasonable steps to ensure that Data Processors:

- **Only process personal data on authorised instructions;**
- **Maintain appropriate confidentiality;**
- **Implement appropriate security measures;**
- **Assist the Company with applicable data protection obligations;**
- **Report personal data breaches promptly; and**
- **Delete or return personal data where required.**

---

21. CHANGES TO THIS POLICY

21.1

The Company reserves the right to amend this Policy where necessary to reflect:

- **Changes in legislation;**
- **Changes in regulatory guidance;**
- **Changes to Company structure;**
- **Changes in business activities;**
- **Changes in information systems;**
- **Changes in data processing activities;**
- **Identified risks or incidents; or**
- **Improvements to the Company's data protection arrangements.**

21.2

This Policy will be reviewed at least annually and sooner where significant changes occur.

21.3

The current approved version of this Policy will be made available to relevant employees and workers.

APPROVAL
Signed by the Compliance Director

Tim Croxford
Date: 07/06/2026