MM-EYE LTD – DATA PROTECTION, SECURITY & DATA MANAGEMENT POLICIES

PART A – COMPANY DATA PROTECTION POLICY

1. POLICY PURPOSE

This Data Protection Policy sets out MM-Eye Ltd.'s commitment to protecting the personal data of employees, customers, suppliers, respondents, stakeholders and other interested parties.

We are committed to handling personal data lawfully, fairly and transparently, and in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018**.**

2. GENERAL PROVISIONS

- This policy applies to all personal data processed by MM-Eye Ltd.
- The **Data Protection Officer (DPO)** has responsibility for ongoing compliance.
- MM-Eye Ltd is registered with the Information Commissioner's Office (ICO).
- This policy is reviewed annually by the Board of Directors.

Current DPO: Deborah Fitzpatrick, Deputy Managing Director
Next scheduled review: January 2027

3. SCOPE

This policy applies to:

- Employees and job applicants
- Contractors, consultants and partners
- Customers, suppliers and research respondents
- Any third party acting on behalf of MM-Eye Ltd

4. DATA PROTECTION PRINCIPLES

MM-Eye Ltd processes personal data in line with Article 5 of the UK GDPR. Personal data shall be:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date

Registered Office:
82 St. John Street London
EC1M 4JN
Registered Number
6379175

- Retained only for as long as necessary
- Processed securely using appropriate technical and organisational measures

5. LAWFUL Bases for Processing

All personal data processed by MM-Eye Ltd must rely on at least one lawful basis:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Where consent is used, clear opt-in consent will be recorded, and individuals will be able to withdraw consent at any time.

6. INDIVIDUAL RIGHTS

MM-Eye Ltd respects individuals' rights under the UK GDPR, including the right to:

- Be informed
- Access their data
- Rectification
- Erasure
- Restriction of processing
- Data portability
- Object to processing

Requests can be made via the Privacy Policy or directly to the DPO.

7. DATA HANDLING RULES

Personal data must:

- Be accurate and up to date
- Be processed only for lawful purposes
- Be protected against unauthorised access

Personal data must not:

- Be shared informally

Registered Office:
82 St. John Street London
EC1M 4JN
Registered Number
6379175

- Be retained longer than necessary
- Be transferred outside the UK without appropriate safeguards .

8. DATA BREACH MANAGEMENT

In the event of a personal data breach, MM-Eye Ltd will:

- Assess the risk to individuals' rights and freedoms
- Notify the ICO within 72 hours where required
- Notify affected individuals where there is a high risk

All suspected breaches must be reported immediately to the DPO.

PART B – DATA & NETWORK SECURITY POLICY

9. PURPOSE

This policy aims to protect confidential and sensitive data from accidental or unlawful loss, misuse or compromise while ensuring employees can access information required to perform their roles.

10. SCOPE

This policy applies to:

- All personal and customer data
- All company IT systems, networks and devices
- All employees, contractors and third parties with system access

11. ACCESS CONTROLS

- Unique user IDs are assigned to all users
- Access follows the principle of least privilege
- Access is revoked immediately upon termination
- Shared accounts are limited to approved service or training accounts

External IT Provider: Curo (responsible for network security and access management)

12. AUTHENTICATION & REMOTE ACCESS

- Remote access is permitted only via approved VPN authentication
- Passwords must remain confidential and not be shared
- Sensitive systems may require multi-factor authentication.

Registered Office:
82 St. John Street London
EC1M 4JN
Registered Number
6379175

13. SECURITY MONITORING & INCIDENTS

- Access logs may be used for investigations
- Curo is responsible for identifying security incidents
- All incidents are escalated to the DPO and Board where appropriate

PART C – ASSET MANAGEMENT POLICY

14. PURPOSE

To ensure hardware and software assets remain secure, supported and fit for purpose.

15. ASSET CONTROLS

- Employees are provided with appropriate hardware and software
- Curo provides a bi-annual asset inventory
- Hardware is replaced at end-of-life or warranty expiry
- All assets must be returned on termination

PART D – DATA STORAGE POLICY

16. PURPOSE

To ensure secure storage, retrieval, archiving and destruction of company data in compliance with legal and contractual obligations.

17. STORAGE PRINCIPLES

MM-Eye Ltd will:

- Store data securely (physical and electronic)
- Restrict use of personal storage devices without authorisation
- Encrypt data where appropriate
- Conduct regular backups
- Review storage capacity and security regularly

PART E – DATA RETENTION & DESTRUCTION SCHEDULE

Data Type	Retention Period
Staff personal documents (passport, photos)	3 months after leaving

Registered Office:
82 St. John Street London
EC1M 4JN
Registered Number
6379175

Client/customer samples	Upon project completion
Recruitment materials	6 months post completion
Respondent photographs	3 months post project completion
Incentive payment details	Immediately after payment
Transcripts	Approx. 3 months post project completion

Data is securely destroyed or anonymised once retention periods expire.

Registered Office:
82 St. John Street London
EC1M 4JN
Registered Number
6379175