General Data Protection Regulation Policy

(Revised February 2026)

Glossary of Terms

MCL: Millbeck Communications Limited
Data Breach: The intentional or unintentional release of secure or private/confidential information to an untrusted environment.
Data Controller: Any person or entity which determines the purposes and manner in which any personal data is processed.
Data Processor: Any person who processes data on behalf of the data controller.
Data Protection Impact Assessment (DPIA): An assessment to identify and minimize data protection risks where processing is likely to result in high risk to individuals' interests.
DPO: The Data Protection Officer appointed to monitor internal compliance and act as a contact point for data subjects and the Information Commission.
Data Subject: The individual who is the subject of personal data.
UK GDPR: The UK General Data Protection Regulation (as amended by the Data (Use and Access) Act 2025).
Information Commission: Formerly the ICO, the UK's supervisory authority for data protection.
OMG: MCL's Operational Management Group.
Personal Data: Any information relating to an identified or identifiable person.
Recognised Legitimate Interest: Specific processing purposes defined under the 2025 Act (e.g., crime prevention) that do not require a balancing test.

1. Introduction

1.1 This policy sets out how MCL will handle personal data in the course of its business and comply with the principles set out in the UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

1.2 The purpose of this policy is to ensure that personal data is processed lawfully, fairly, and transparently, protecting the rights and freedoms of all individuals whose data we hold.

2. Data Protection Principles

2.1 MCL is committed to processing data in accordance with the following principles. Personal data shall be:

1. Processed lawfully, fairly, and in a transparent manner.
2. Collected for specified, explicit, and legitimate purposes.

3. Adequate, relevant, and limited to what is necessary.
4. Accurate and kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary.
6. Processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss.
7. Data Protection Officer (DPO)

3.1 MCL shall appoint a DPO, who shall be a Director.

3.2 The DPO is responsible for responding to enquiries, monitoring compliance, and maintaining registers for processing activities, data breaches, and DPIAs.

3.3 The DPO shall report data breaches to the Information Commission when the legal threshold for reporting is met.

4. Lawful, Fair and Transparent Processing

4.1 All data processed by MCL must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public duty, or legitimate interests. 4.2 Recognised Legitimate Interests: In accordance with 2025 reforms, MCL may process data without a formal balancing test where it is necessary for recognised purposes such as the prevention of crime, safeguarding, or responding to emergencies. 4.3 Consent: Where consent is relied upon, it must be clear and freely given. Individuals have the right to revoke consent at any time.

5. Retention & Destruction

5.1 MCL shall maintain a Retention & Destruction policy. Data will be held no longer than is necessary, determined by statutory requirements, industry best practice, and operational needs.

5.2 Secure Destruction: Personal data must be destroyed securely (e.g., shredding or secure digital deletion) to ensure it is put beyond use.

6. Data Security

6.1 MCL shall implement robust technical and organizational measures to protect data. These measures are reviewed periodically to ensure they remain commensurate with modern security risks. 6.2 Portable equipment and removable media shall not be used to store personal data. Work on laptops must be conducted via remote, password-protected logins to MCL servers.

7. Data Requests and SARs

7.1 Subject Access Requests (SARs): Individuals have a right to access their data. MCL will respond within one calendar month. 7.2 Clarification and "Stop the Clock": Under the 2025 Act, if a request is broad, MCL may pause the response period to seek clarification. The timer restarts once the requester provides the necessary details. 7.3 Reasonable Search: MCL is required to conduct a reasonable and proportionate search for data but is not required to undertake searches that impose an abusive or excessive burden.

8. Internal Complaints Procedure (2026 Statutory Requirement)

8.1 MCL maintains a formal internal complaints procedure for data protection matters. 8.2 Any individual who believes their data rights have been infringed must lodge a complaint with MCL first.

8.3 MCL will acknowledge all data protection complaints within 30 days and conduct an investigation without undue delay.

8.4 Escalation: If an individual remains dissatisfied after the internal investigation, they may escalate the matter to the Information Commission.

9. Data Breaches

9.1 Any person aware of a data breach must immediately inform the DPO.

9.2 The DPO will assess the risk to individuals' rights and, where appropriate, report the breach to the Information Commission within 72 hours.

10. Data Protection Impact Assessments (DPIA)

10.1 A DPIA must be carried out for any high-risk processing, such as extensive profiling, adopting innovative technologies, or processing sensitive data in a new way.