DATA PROTECTION POLICY

Effective Date	1 May 2022		
Accountable Department	Corporate		
Policy Number	CORP_17_v01_2022	**Version**	1
Applicability	All employees, agents, consultants, volunteers, and other representatives of m2m. In addition, employees and representatives of partner agencies (subrecipients, subcontractors, suppliers/vendors) who have a formal relationship with m2m.		

I. PURPOSE

Ensuring data protection is the foundation of trustworthy business and research relationships and essential to protecting the reputation of mothers2mothers (m2m). m2m is committed to compliance with data protection laws and international data protection standards. This Data Protection Policy applies to all m2m branches and entities and is based on globally accepted, basic principles of data protection.

II. SCOPE OF THE POLICY

This Data Protection Policy applies to all m2m employees. This Policy applies to all personal information handled by m2m, both data held tangibly/physically or electronically. So long as the processing of the personal information is carried out for m2m purposes, this Policy applies regardless of where the personal information is held. For example, this Policy covers personal information held both at m2m offices and on mobile devices (such as electronic notebooks or laptops) that may be used by employees or other third parties outside of m2m offices. This Policy also applies regardless of who owns the device on which m2m personal information is stored.

III. APPLICATION OF NATIONAL LAWS

The Data Protection Policy comprises internationally accepted data privacy principles without replacing existing national laws. Relevant national laws will take precedence in the event that it conflicts with the Data Protection Policy, or has stricter requirements.

Each m2m entity or branch is responsible for compliance with m2m's Data Protection Policy and the legal obligations of the country in which they operate. If there is reason to believe that legal obligations contradict the duties under this Policy, the relevant branch or entity must inform m2m's Chief Operating Officer (COO) and m2m's Information Officer. In the event of conflicts between national legislation and this Policy, the COO will work with the relevant branch or entity to find a practical solution that meets the purpose of this Policy and relevant legal requirements.

IV. KEY DEFINITIONS

a) *Biometrics:* A technique of personal identification that is based on physical or behavioural characterisations including fingerprinting, retinal scanning, and voice recognition.
b) *Child:* Any person who has not attained 18 years of age regardless of the age of majority or age of consent locally.
c) *Data Subject:* The person (or juristic person) to whom the personal information relates.

d) De-identify: The deletion of any information that: (1) identifies a Data Subject; (2) can be used or manipulated by a reasonably foreseeable method to identify a Data Subject; or (3) can be linked by a reasonably foreseeable method to other information that identifies a Data Subject.

e) *Juristic Person:* A juristic person is a non-human legal entity recognized by the law and entitled to rights and duties in the same way as a human being.

f) *Personal information*: Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to the following:

1. Information relating to the gender, sex, marital status, disability, language, and birth of a person;
2. Information related to the educational, financial, or employment history of a person;
3. Any identifying number or symbol such as ID or passport numbers;
4. Contact or other location information such as email addresses, physical addresses, or telephone numbers;
5. The personal opinions, views, or preferences of a person;
6. The opinions or views of one individual about another individual; and
7. Correspondence sent by a person that is implicitly or explicitly of a private and confidential nature.

g) *Processing*: Processing data is widely defined and includes any operation or activity, whether or not by automatic means, involving personal information, including the following:

1. Collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
2. Merging, linking, or dissemination by means of transmission, distribution, or making available in any other form; or
3. Restriction, degradation, erasure, or destruction of information.

h) *Special Personal information*: Personal data consisting of information relating to:

1. The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, or biometric information of a Data Subject; and
2. The criminal behaviour of a Data Subject to the extent that such information relates to either the alleged commission of an offence or any proceedings in respect to an offence allegedly committed by a Data Subject.

i) *Confidential Data*: Data given in confidence or data agreed to be kept confidential. In other words, information that is not in the public domain.

V. KEY PRINCIPLES

Any employee using personal information must comply with the following data protection principles as they define how personal information can be legally processed:

a) *Accountability*: Personal information must be obtained and processed fairly and lawfully and with the consent of the Data Subject.
b) *Purpose Specification*: Personal information must be obtained for a specific, defined, and lawful purpose.
c) *Processing Limitations*: Personal information may not be processed for a secondary purpose unless compatible with the original purpose or with the consent of the Data Subject. Personal information must not be kept for longer than is necessary.
d) *Information Quality*: Personal information must be adequate, relevant, and not excessive. It must also be accurate and updated when necessary.
e) *Openness*: Personal information must be processed in accordance with the Data Subject's rights and the Data Subject must be aware that their personal information is being collected and for what purpose the information will be used.
f) *Security Safeguards*: Personal information must be kept secure against the risk of unauthorised access, modification, accidental loss, unauthorised destruction, or disclosure. Personal information must not be transferred outside the country of collection unless the receiving country has equivalent levels of protection for personal information.
g) *Data Subject Participation*: Data Subjects may request to know what personal information is held about them and request that their personal information be corrected and/or deleted.

VI. DATA SECURITY

Keeping personal information secure is key to complying with international data protection standards. All m2m employees are responsible for ensuring that personal information is kept secure and not disclosed (either orally, in writing, or accidentally) to any unauthorised third party.

At a minimum, m2m employees will take the following steps to secure personal information:

1. Ensure that any personal information recorded in paper form or hard copy documents is kept in locked filing cabinets or locked drawers or locked offices. Paper and hard copy documents containing personal information should never be left in public areas where they can be accessed by unauthorised individuals, lost, misplaced, or damaged.

2. Ensure that the same measures are taken in regards to any storage devices such as discs, memory sticks, USB drives, or similar devices on which personal information is held.
3. Ensure that if any personal information is held on a mobile device that it is properly password protected and, where appropriate, encrypted.
4. Ensure special care is taken whenever personal information is transferred from one place to another to ensure the security of the data.
5. Ensure that access to personal information is only granted to m2m employees who require it for legitimate business purposes.
6. Report data security breaches or potential breaches immediately to the m2m IT Department and the m2m Information Officer. This includes lost or stolen laptops, tablets, data storage devices or other mobile devices, or the accidental disclosure of personal information, such as sending an email with personal information or other confidential data to the wrong recipient.
7. Whenever possible, de-identify personal information to avoid the unintentional identification of a Data Subject.
8. Person information that is no longer needed or in use must be permanently deleted or destroyed in a manner that cannot be reasonably reconstructed.

The following actions are always prohibited when handling personal information:

1. Using personal information obtained for one purpose for another supplemental purpose without appropriate consent.
2. Disclosing personal information to a third person or party outside of m2m without the consent of the Data Subject and/or consultation with the m2m Information Officer.
3. Collecting the personal information of children without the documented consent of their parent or legal guardian.

VII. RESEARCH - SPECIAL CONSIDERATIONS

Before commencing any research, which will involve obtaining or using Personal information, the employee conducting the research and their supervisor or Head of Department must give due consideration to this Policy and relevant data privacy laws and compliance with such laws.

In particular, employees will need to consider the type of personal information which may be collated, how consent is to be recorded, the extent to which such data may legitimately be required for the research objective, how the data will be securely stored, and the duration for which data will be retained.

Personal information obtained or used for research should be limited to the minimum amount of data reasonably required to achieve the desired research objectives, and, wherever possible, any such personal information should be de-identified.

VIII. CONSEQUENCES OF BREACHING THIS POLICY

Any breach of this Policy will be considered a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Policy may also result in m2m and/or the individual being held liable under local law.

Anyone with concerns about how m2m is processing personal information or confidential data may report their concerns to the m2m Information Officer at privacy@m2m.org or anonymously by writing to whistleblower@m2m.org.

Approved and Reviewed by:

Name	Title/Department	Signature	Date
Frank Beadle de Palomo	President & Chief Executive Officer	DocuSigned by: Frank Beadle de Palomo B89E8EDF77014E9...	May 23, 2022

Related Policy(ies)/Procedures	Privacy Policy IT and Social Communications Policy
Source/Reference	Data Protection Act 1998: http://www.legislation.gov.uk/ukpga/1998/29/contents Protection of Personal Information Act, 2013: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf The General Data Protection Regulation (GDPR) https://gdpr.eu/tag/gdpr/