

GDPR & Data Protection Policy

Version 07 – Effective from 3rd November 2026
Next review due: 3rd November 2027
Approved by: Mama2Mama Board of Trustees

Status: Approved by Board of Trustees.

Organisation: Mama2Mama Baby Essentials CIO • Registered charity 1199777

Policy owner and primary contact: Zuzana Fratrikova, Founder & CEO | info@mama2mama.org.uk

Approval date: 3rd November 2026 | **Approved by:** Board of Trustees

1. Why this policy matters

At Mama2Mama, trust is everything. Families come to us at vulnerable points in their lives, and when they do, they often share sensitive information about themselves and their children. That trust is never taken for granted.

This policy explains what personal information we collect, why we use it, how we protect it, how long we retain it, and how individuals can exercise their rights. It reflects the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and our dignity-first values. Behind every piece of data is a real person; protecting their information is part of protecting their dignity.

This policy applies to trustees, employees, volunteers, contractors and authorised partners handling data for Mama2Mama, including activity at Café 51 Community Hub, the Shurgard Donation Warehouse Unit, referrals, collections, events and online services.

2. Accountability and responsibilities

Mama2Mama acts as a controller for personal information it determines the purposes and means of processing. Where another organisation determines its own purposes, its controller responsibilities remain separate; any joint-controller arrangement must be documented.

The Board of Trustees is accountable for oversight, resources and approval. Zuzana Fratrikova, Founder & CEO, is the Data Protection Lead and primary contact for requests, incidents, training coordination and maintaining records. This title does not assert that a statutory Data Protection Officer has been appointed; whether a formal DPO is legally required must be assessed and recorded.

Every staff member, volunteer and contractor must protect information, use only authorised systems, follow instructions, report incidents promptly and respect confidentiality after leaving. The independent trustee contact for complaints or concerns involving the CEO is Miroslava Zverbikova, Chair of Trustees (zverbikovam@yahoo.com).

3. Data we may collect and why

Family and referral information: names, contact details, children's ages, household circumstances, needs, referral source, support provided and follow-up notes. Sensitive details (for example health, disability, domestic abuse or immigration-related information) must be collected only when genuinely necessary and with enhanced safeguards.

Staff, trustee and volunteer information: recruitment, contact and emergency details, role and training records, payroll where relevant, safeguarding and DBS status only to the extent lawful and necessary. **Donor, funder and partner information:** contact details, donations, Gift Aid declarations, correspondence and reporting records.

Café 51 and community activities: bookings, attendance, event and customer enquiries, accessibility or allergy requirements when relevant, payment transaction records and consent-based photographs or stories.

Payment-card details must be handled by approved payment providers; do not retain full card details locally.

We collect only information needed for a defined purpose, explain that purpose at collection, and avoid unnecessary copies or excessive case notes.

4. Lawful bases and sensitive information

No single lawful basis applies to all processing. Before collecting or reusing information, the Data Protection Lead will record the relevant Article 6 lawful basis by purpose, such as legitimate interests (after balancing assessment), legal obligation, contract, consent, or vital interests where appropriate. Consent is not automatically the correct basis for core referrals or safeguarding.

Where special-category information is processed, an Article 9 condition and any applicable Data Protection Act 2018 Schedule 1 condition must also be identified, with an appropriate policy document where legally required. Criminal-offence/DBS information requires its own lawful authority and restrictions. Staff must not assume a general consent form makes all sensitive processing lawful.

Photography, testimonials and identifiable publicity require clear, specific permission, including suitable parental responsibility arrangements for children. Refusal must never affect access to support. Consent withdrawal stops future consent-based use, subject to any lawful exceptions and practical limitations for material already distributed.

5. Data protection principles

We process data lawfully, fairly and transparently; collect it for specified purposes; minimise what we collect; keep it accurate; retain it no longer than necessary; protect it with appropriate security; and demonstrate accountability through records, training and reviews.

We will provide accessible privacy information to families, staff, volunteers, donors, referrers and Café 51 users at or before collection, with additional explanation when information is obtained indirectly or used for a new purpose.

6. Referral handling, safeguarding and information sharing

Professional referrals are accepted through approved channels. Referrers should send only necessary information, confirm that the person has been informed where appropriate, and use secure transmission. Access to referral and safeguarding records is restricted to authorised personnel with a genuine need to know.

Information may be shared with health visitors, social workers, housing professionals, safeguarding agencies or other partners where a lawful basis and appropriate safeguards exist. Consent may be sought when appropriate but is not always required or suitable for safeguarding. Disclosures must be necessary, proportionate, recorded and made securely; do not promise absolute confidentiality where someone may be at risk.

Where possible, share anonymised or properly aggregated information with funders. Identifiable case studies or reporting require an identified lawful basis, transparency and controls. Formal processor agreements, data-sharing arrangements and transfer checks must be established as applicable.

7. Security, access and devices

Approved systems must use role-based access, strong unique passwords and multi-factor authentication wherever supported. Permissions are granted by role, reviewed when duties change and removed promptly when someone leaves. Confidential records must not be accessed from shared or unsecured devices.

Use approved cloud storage and organisational accounts. Do not send referral details to personal email, personal messaging groups or unauthorised apps; do not save client records on personal devices or removable media without explicit written approval and protective controls. Verify recipients before sending sensitive information and use secure transfer methods.

Paper records must be minimised, kept in locked storage accessible only to authorised people, transported securely and shredded when due for disposal. Screens must be locked when unattended. Report missing devices, misdirected emails, suspicious links and unauthorised access immediately.

Third-party software, event-booking services, payment systems and cloud providers must be assessed for privacy and security; written processor terms and international transfer safeguards are required where applicable.

8. Café 51, events, photography and marketing

For Café 51 bookings and events, collect only information necessary to manage reservations, safety, payment and reasonable adjustments. Allergy and disability details should be accessed only by staff who need them and deleted according to the retention schedule.

Clearly distinguish operational booking messages from optional marketing. Electronic marketing must comply with applicable PECR and data protection requirements, including consent or another valid route where available and a simple opt-out. Do not add café customers, donors or families to marketing lists merely because they used a service.

Photographs or recordings at the café, workshops and children's events require an appropriate notice and permissions; staff and volunteers must not take or post identifiable images of families without authorisation.

9. Individual rights and requests

Individuals may have rights to be informed, access, rectification, erasure, restriction, portability, objection and protections relating to solely automated decisions, subject to legal conditions and exemptions. Requests can be made verbally or in writing to info@mama2mama.org.uk and must be passed immediately to the Data Protection Lead.

We will verify identity proportionately, log the request, assess applicable rights and respond without undue delay and normally within one calendar month. Lawful extensions of up to two additional months may apply for complex or multiple requests, with timely notice. Do not routinely charge; a reasonable fee or refusal is permitted only in circumstances allowed by law.

If someone is unhappy, they may complain to Mama2Mama or the Information Commissioner's Office (ICO). Requests involving the CEO can be escalated to the independent trustee contact, Miroslava Zverbikova, Chair of Trustees.

10. Retention, disposal and legal holds

Retain information only for documented periods justified by purpose, legal obligations and risk. Indicative periods are up to three years after last family contact, six years after volunteer/staff departure and seven years for financial/grant documents; these are starting points, not blanket legal rules. See the retention schedule in Appendix A.

Safeguarding, employment, payroll, Gift Aid, incident, children's and litigation-related records may require different periods. The Data Protection Lead must approve a verified schedule, document exceptions and suspend deletion where a complaint, investigation or legal hold requires preservation.

At the end of retention, delete electronic data securely, dispose of paper confidentially and remove access to backups according to documented technical capability and backup cycles.

11. Personal data breaches and incident response

Anyone who suspects loss, unauthorised disclosure, alteration, destruction, ransomware or access to personal data must report it to Zuzana Fratrikova immediately, including outside normal hours where serious. Do not conceal an incident or investigate by accessing records beyond your authority.

The Data Protection Lead will contain the incident, preserve evidence, record when it was discovered, assess the likelihood and severity of risk, and decide on notification. A breach that is likely to result in a risk to individuals' rights and freedoms must be reported to the ICO without undue delay and, where feasible, within 72 hours of awareness; if delayed, reasons must be given. High-risk breaches must also be communicated to affected individuals without undue delay unless an exception applies.

All incidents and near misses are logged with actions, owners, outcomes and lessons learned, including those not notifiable to the ICO. Where the CEO is implicated or unavailable, escalation goes to the independent trustee.

12. Training, assessments and assurance

All personnel with access to personal data receive induction appropriate to their role, confidentiality instructions and periodic refreshers. Higher-risk roles receive additional training on referrals, safeguarding, subject access requests and incident response.

Maintain a record of processing activities where required, lawful-basis decisions, legitimate-interest assessments where used, a data-sharing/processor register, access reviews and a privacy-notice inventory. Conduct a Data Protection Impact Assessment before processing likely to create high risk, such as new sensitive-data systems or large-scale monitoring. Review any CCTV separately for necessity, notices, retention and access if installed.

Assess whether an ICO data protection fee is payable and verify the organisation's registration and contact details. Review this policy annually and sooner after material changes, incidents or legal updates.

13. Monitoring and trustee oversight

The Data Protection Lead will provide trustees with proportionate assurance on training, rights requests, breaches, processor checks, retention and outstanding actions without unnecessarily exposing personal information. The Board will review significant incidents and approve necessary improvements.

This policy sets the required standards. Implementation checks are listed in Appendix B, and progress is reported to trustees.

Appendix A — Retention schedule

Record type	Indicative period	Decision / qualification
Family referral / support	Up to 3 years from last contact	Verify safeguarding exceptions, funder terms and necessity
Safeguarding concerns	Separate schedule required	Determine applicable statutory guidance, case type and risk
Volunteer files	Up to 6 years after leaving	Check contents; DBS details kept only as legally permitted
Staff / payroll	Category-specific; often 6 years or more	Confirm employment, pension, tax and legal requirements
Financial / grant	Often 6–7 years	Confirm HMRC, Gift Aid, grant and audit rules
Café bookings / events	Set proportionate period	Separate payment, safety and marketing records
Media consent / images	Purpose-specific	Record permission, review use, honour withdrawal where applicable
Data incidents / rights requests	Set documented period	Consider accountability and potential claims

Appendix B — Implementation and verification checklist

- [ ] Confirm whether a statutory DPO is required and publish the independent trustee escalation contact (Miroslava Zverbikova, Chair of Trustees).
- [ ] Verify ICO registration / fee status and update contact details.
- [ ] Map actual data systems and processors (referrals, cloud files, email, payments, Café 51 events and marketing).
- [ ] Approve role-specific lawful bases, special-category conditions and accessible privacy notices.
- [ ] Confirm written processor agreements, data-sharing arrangements and any international transfers.
- [ ] Review access rights, MFA, device controls, backups and paper storage at current premises.
- [ ] Approve category-specific retention schedule, deletion procedures and safeguarding exceptions.
- [ ] Create and test breach register, 72-hour escalation procedure and subject access request log.
- [ ] Check photo permissions, children's consent processes and electronic marketing compliance.
- [ ] Complete staff/volunteer training, confirm owners and schedule annual assurance report.

Approval record

Board approval date:	3rd November 2026
Policy lead:	Zuzana Fratrikova, Founder & CEO
Next scheduled review:	3rd November 2027

Miroslava Zverbikova

Miroslava Zverbikova
Chair of Trustees
Signed electronically on 3rd November 2026

Agnieszka Derejska

Agnieszka Derejska
Trustee
Signed electronically on 3rd November 2026

Hazel Chawapiwa

Hazel Chawapiwa
Trustee
Signed electronically on 3rd November 2026

Roy Gopaul

Roy Gopaul
Trustee
Signed electronically on 3rd November 2026

Zuzana Fratrikova

Zuzana Fratrikova
Policy owner · Founder & CEO
Signed electronically on 3rd November 2026

Trust is everything.
Every family matters.

Families come to us at vulnerable points in their lives, and when they do, they often share sensitive information about themselves and their children. That trust is never taken for granted.

Behind every piece of data is a real person; protecting their information is part of protecting their dignity.

If you have a question or a request about your personal information, contact us at info@mama2mama.org.uk.



Mama2Mama Baby Essentials 51 Powis Street, London SE18 6HZ info@mama2mama.org.uk