London Sperm Bank

Personal Data Privacy, Protection & Confidentiality

Definitions

For the purpose of this policy the following terms are used:

- **A data controller** is the entity that determines the purposes and means of processing personal data and is ultimately responsible for ensuring compliance with data protection laws.
- **The Data Protection Act (DPA)** is UK legislation that governs how personal data is collected, used, stored, and shared, ensuring individuals' information is handled fairly, safely, and transparently.
- **A Data Protection Officer (DPO**) is a professional responsible for ensuring that an organization complies with data protection laws and regulations.
- **The General Data Protection Regulation (GDPR)** is the European Union's comprehensive law designed to protect personal data and privacy for individuals within the EU, applying to organizations worldwide that handle EU residents' data.
- **The Human Fertilisation and Embryology Authority HFEA** are the UK's independent regulator of fertility treatment and research using human embryos.
- **London Sperm Bank (LSB**) are the UK registered company (05925090) providing a service.
- **J D Healthcare (JDH)** are a UK registered company (05919836) wholly owning LSB.

Identity and contact details of the controller

In this Privacy policy we use **"we"** or **"us"** or **"our"** or **"LSB"** to refer to the London Sperm Bank, a registered company. Our principal place of business is 1 St Thomas Street, London, SE1 9RY. We are contactable at this address, as well as by telephone on +44 (0) 20 7563 4305, or email: info@londonspermbank.com

Our Data Protection Officer ("DPO") helps ensure that LSB complies with data protection law. Our DPO has responsibility for data protection compliance. The DPO can be contacted by email at LSB-DPO@londonspermbank.com or post to: Data Protection Officer, London Sperm Bank, 1 St Thomas Street, London, SE1 9RY.

If you would like further information about any of the matters in this Privacy Policy or have any other questions about how we collect, store or use your personal information, please contact the DPO using the details above.

Policy Statement

At London Sperm Bank (LSB), we are committed to providing clear guidance and consistent standards in relation to personal, sensitive, genetic, and confidential information being handled safely, lawfully, and ethically, protecting your privacy, confidentiality, and personal information.

We process sensitive data, including donor and medical information, and we follow strict legal and ethical rules to keep it safe. This policy outlines what information we collect, how we use it, and the steps we take to protect your privacy, the principles, responsibilities, and relevant standard operating procedures (SOPs) to be followed to ensure compliance with relevant legislation and to support fair and transparent treatment for all employees, patients, partners, donors and suppliers.

It defines the complete governance, data-protection, confidentiality, and information-security framework used by LSB and applies to every stage of information handling; collection, storage, access, transfer, use, retention, and deletion, across donor recruitment, screening, matching, laboratory procedures, customer support, digital systems, and exports/imports.

Please take your time to read this policy carefully.

Scope

This policy applies to donors and prospective donors, clients purchasing donor samples, clients using the Matching Service (including photo submissions), website visitors who submit enquiries or forms, contractors, laboratories, screening partners, couriers, and IT providers, anyone with authorised access to LSB confidential information and all LSB and J D Healthcare employees, including those on full-time, part-time, fixed term, and temporary contracts, unless otherwise stated.

This policy explains how we collect, use, store, share, and protect personal information across all LSB services. It applies to anyone whose information we process, and to everyone working with or on behalf of LSB and sets out the rules, responsibilities, and governance requirements that apply to all personal, sensitive, genetic, and confidential information processed by LSB. It covers all individuals, systems, and organisations involved in donor recruitment, medical screening, matching services, laboratory workflows, administrative processing, exports/imports, website interaction, record-keeping, and digital communication.

Regulations

LSB has formulated this policy to facilitate compliance with its legal obligations under UK GDPR, the Data Protection Act 2018, the Human Fertilisation and Embryology Act (HFEA), the HFEA Code of Practice, ICO requirements, LSBs DPIAs and ISO 9001:2015 information-security obligations and quality management requirements.

We follow strict HFEA donor anonymity rules, your information is kept secure and only used for clear, lawful purposes and we never use your data for marketing without consent.

Objectives

LSB have set clear objectives and purpose of this policy to ensure:

- Lawful and transparent processing of all personal data
- Protection of confidentiality, integrity, and data availability
- Compliance with HFEA donor anonymity rules
- Proper management of special-category and genetic data
- Strong information security aligned with ISO 9001
- Clear accountability for all individuals handling LSB data

How We Keep Your Information Confidential

London Sperm Bank takes the privacy, protection and confidentiality of your information very seriously. We aim to meet current Internet best practice and adhere to UK data protection laws.

LSB enforces strict confidentiality obligations to protect all donor, client, laboratory, and operational information. These obligations apply to employees, contractors, third-party processors, and temporary workers, and remain in place even after the working

relationship ends. No identifying donor, client, or internal operational information may be disclosed without explicit authorisation and a lawful basis.

Staff Confidentiality Requirements:

- Access only the information required for assigned duties ("need-to-know")
- Use only approved secure communication systems
- Follow password, encryption, and access-control rules
- Ensure all confidential files are stored securely
- Prevent unauthorised viewing, overhearing, or access
- Never store data on personal devices or messaging apps
- Report suspected or confirmed breaches immediately

Confidential Information Includes:

- Donor identities and anonymity information
- Genetic and medical screening results
- Optional photographs submitted for matching
- Counselling and eligibility assessment records
- Client contact information and payment details
- Laboratory data and operational quality documents

What Information We Collect & Process

We only collect information we genuinely need to provide safe, high-quality services and meet regulatory requirements. Due to the nature of our services, you will be asked to submit personal information about yourself in order to receive or use our services. By completing our online enquiries forms, live chat forms or providing information to us via email or phone, you are giving consent for us to store and use this information to provide you with the best possible service.

LSB processes several categories of personal and special-category data. Most donor and matching data is highly sensitive, including genetic, medical, and photographic information, requiring enhanced protection, confidentiality, and strict access limitations.

Donor Data:

- Identity and demographic information
- Medical and lifestyle history
- Genetic and infectious disease screening results
- Counselling and eligibility assessments
- Donor profile information used on the website
- Compensation and financial documentation

Matching Service Data:

- Client phenotype preferences
- Optional client-submitted photographs
- Internal phenotype comparison notes

Website & Operational Data

- Enquiry form submissions and emails
- Cookies, analytics, and IP addresses
- Export/import documents
- Courier and shipping records

How We Use Your Information

We use your information only for clear, lawful purposes linked to our regulatory duties, services and specific purposes relating to donor programme administration, regulatory compliance, client-requested services, laboratory operations, and safe service delivery. No automated decision-making or biometric profiling is used.

Data is processed for:

- Donor eligibility, medical screening, and assessment
- Creation of anonymised donor profiles
- Compliance with HFEA Code of Practice
- Provision of donor samples and export/import coordination
- Manual phenotype-based matching
- Responding to enquiries and providing client support
- Maintaining internal audits, accountability logs, and quality records

Our services are designed to give you the information that you want to receive. These services include information about fertility related services, newsletters and competitions, live chats and information relating to appointments and your enquiry. We will also need personal information to help us identify you when you contact us. When we collect this information, we will only do so over a secure connection. We may combine this information with other information that we may hold about you if you are an existing customer or have made enquiries to us before.

If you would like to amend your personal details, please phone us on +44 (0) 20 7563 4305, or email: info@londonspermbank.com

Lawful Basis for Processing

LSB processes personal and special-category data only where a valid lawful basis exists under UK GDPR. Different lawful bases apply depending on whether the data relates to donor screening, laboratory diagnostics, Matching Service activities, client communication, or website usage. Special-category data such as genetic, medical, and health information requires an additional justification under Article 9. All lawful bases are documented in the LSB ROPA and DPIAs, and staff must ensure processing always aligns with these recorded purposes.

Lawful bases used at LSB:

- Legal obligation – HFEA regulatory compliance
- Contract – donor agreements and Matching Service contracts
- Legitimate interests – programme operations, safety, screening, enquiries
- Consent – general enquiries, marketing where applicable
- Explicit consent – processing genetic data or Matching Service photographs
- Vital interests – rare emergencies affecting safety

London Sperm Bank

Information Security Controls (ISO 9001 & GDPR Aligned)

LSB maintains a comprehensive information security framework designed to protect all physical and digital information assets. Security controls are aligned with ISO 9001:2015, GDPR's "Security of Processing" requirements, and sector-specific best practices. All systems used to store, access, or process donor or client data must be encrypted, access-controlled, regularly reviewed, and subject to continuous monitoring. Staff must follow all security SOPs and never bypass or disable security features.

Technical Security Controls:

- Encryption of all data in transit and at rest
- Multi-factor authentication for all sensitive systems
- Role-based access controls (RBAC)
- Device hardening and mandatory anti-malware
- Automatic screen-lock and short timeout settings
- Secure deletion tools for disposal of files
- Controlled backups and disaster-recovery procedures

Operational & ISO Controls:

- Document control in line with ISO 9001 Clause 7.5
- Regular internal audits (ISO Clause 9.2)
- Quality reviews and risk assessments (ISO Clause 6.1)
- Physical access restrictions in lab and storage environments
- Mandatory training and competency assessments (ISO Clause 7.2)

Donor Anonymity (HFEA Requirement)

Donor anonymity is a legal requirement enforced by the Human Fertilisation and Embryology Authority (HFEA). LSB must ensure that donor-identifying information is never released to clients, clinics, the public, or unauthorised parties. Staff must take particular care when handling profile information, laboratory data, email communications, and any documents containing donor identities. Identity release is controlled solely by the HFEA and must never be performed by LSB.

Donor anonymity requirements include:

- No disclosure of donor names or identifying details
- Only non-identifying profiles may be shared externally
- Strict separation of identifying and non-identifying data
- Internal system access limited to essential staff only
- Counselling, laboratory, and screening data must not reveal identity
- HFEA handles all identity release requests at age 18 for post-2005 donors

International Transfers

How LSB Manages Overseas Processing:

Some LSB services require international data transfers, especially for genetic screening performed by overseas laboratories or when donor gametes are exported outside the UK. LSB ensures that all international transfers are protected by appropriate safeguards as

required by UK GDPR. Transfers must only occur under approved contractual mechanisms and with documented transfer risk assessments.

Safeguards used for international transfers include:

- UK IDTA (International Data Transfer Agreement)
- Transfer Risk Assessments (TRA)
- Encryption of all transmitted data
- Contracts with guaranteed GDPR-equivalent protections
- Secure courier systems for physical sample movement

How Long We Keep Information

LSB applies strict data retention schedules based on legal, regulatory, and quality management requirements. Data is retained only for as long as necessary to fulfil the purpose for which it was collected. Once retention periods expire, records must be securely deleted or destroyed. Staff must follow LSB's Retention Schedule and must not retain personal data beyond its required period.

Retention periods:

- Donor Records: **Minimum 10 years** (HFEA requirement)
- Matching Service Photographs: **30 days maximum**
- Client enquiries: **12 months**
- Financial and transaction data: **7 years**
- Quality & audit documentation: **as per ISO retention matrix**
- Export/import documentation: **regulated retention requirements**

Secure deletion methods:

- Encrypted digital wiping
- Removal from backups when required
- Confidential shredding for paper records

Sharing Your Information

LSB shares personal data only where strictly necessary and always under a lawful basis. Data is shared with carefully selected and approved partners who must demonstrate GDPR compliance and strong security controls. Sharing is limited to what is necessary for screening, laboratory processes, exports/imports, regulatory reporting, and service delivery. Donor-identifying data is never shared with clinics, clients, or international partners.

Data may be shared with:

- HFEA (regulatory compliance and audits)
- Accredited laboratories for infectious disease and genetic testing
- Fertility clinics (non-identifying donor profile data only)
- Courier partners for export/import documentation
- Secure IT hosting and support providers
- Legal and regulatory authorities when required

Data is NEVER shared with:

- Clients or recipients (identifying donor information)
- Clinics (identifying information)
- Anyone outside authorised LSB operations

Your Legal Rights

All individuals whose data is processed by LSB have specific rights under UK GDPR. These rights allow individuals to understand, access, correct, restrict, or object to the processing of their personal data. Requests must be handled promptly, transparently, and in accordance with statutory timeframes. LSB must ensure identity verification before releasing information.

Individuals may request:

- Access to their personal data (Subject Access Request)
- Correction of inaccurate or incomplete information
- Deletion (where legally permissible)
- Restriction of processing
- Objection to certain processing activities
- Data portability
- Withdrawal of consent at any time

Breach Management & Reporting

LSB maintains a structured incident-response process aligned with GDPR and ISO requirements. All staff must report any suspected or confirmed breach immediately. The DPO oversees breach investigation, assessment of risk, documentation, and regulatory notifications.

Breach management includes:

- Immediate containment and mitigation
- Investigation and classification of severity
- ICO notification within 72 hours (if required)
- HFEA reporting where applicable
- Corrective action and root cause analysis
- Updates to SOPs and training as required

Fingerprint ID

London Sperm Bank uses a biometric fingerprint scanning system (RI Witness® Cooper Surgical) to securely verify donor identity and to ensure accurate traceability of all samples collected during the donation process. This measure supports compliance with HFEA traceability requirements and safeguards against sample mix-ups.

The system records an encrypted digital code (“template”) generated from your fingerprint. It does not capture or store an image of your fingerprint. The data cannot be used to recreate your fingerprint or identify you outside the clinic.

Your fingerprint template is linked to your donor record and used only:

- to confirm your identity during clinic visits,
- to track and verify samples collected under your donor ID, and

- to comply with traceability standards for the storage and use of human tissue and gametes.

Your biometric data is stored securely within the RI Witness system on London Sperm Bank's on-premises server, is not transmitted outside the clinic's network and is accessible only to authorised personnel. It is not saved or shared externally or used for any marketing or research purposes.

Optional Photograph Processing (Matching Service)

Clients may voluntarily submit a photograph to support manual phenotype comparison. Photograph processing is strictly controlled, subject to explicit consent, and used only for matching purposes.

Photograph processing rules:

- Photographs processed only with explicit documented consent
- Used solely for manual phenotype comparison by trained staff
- Never analysed using biometrics, AI, or automated tools
- Never shared externally
- Stored securely in encrypted folders with restricted access
- Deleted within 30 days after service completion

CCTV Monitoring

We operate CCTV cameras in public and communal areas of our premises for safety, security, and crime prevention purposes. Cameras are clearly signposted, and footage may capture individuals in these areas, including patients and visitors. All footage is stored securely, with access limited to authorised personnel only. CCTV data is processed under our legitimate interests and in compliance with UK data protection laws, including the Data Protection Act 2018 and UK GDPR.

Comminication

The Company will ensure that all persons employed either as direct employees or contractors are provided with all relevant information related to privacy, data protection and confidentiality, The Management of the Company will consult with the employees (where relevant) on all relevant matters of this policy and arrangements and will ensure staff are kept informed of any changes that are made to relevant procedures.

Training & Compliance

All LSB staff receive mandatory training to ensure they understand their responsibilities under GDPR, HFEA rules, confidentiality expectations, information security controls, and ISO requirements.

Upon commencement of employment all employees (where relevant) will be given training on:

- GDPR & confidentiality
- HFEA Code of Practice
- Information security & data handling
- Fingerprint ID (where relevant)
- Matching Service photo-handling (where relevant)
- Quality management & SOP adherence

All LSB staff will receive refresher training as appropriate with competency monitored and documented.

All employees will be instructed to report any incorrect or non-complaint processes to their line manager.

All employees will receive instruction on their role in relation to this policy.

Further training may be required if there are any changes that may affect this policy. All training will be provided during normal working hours.

Records

This policy forms part of the LSB Quality Management System. It is subject to version control, annual review, and routine internal audits to ensure compliance with GDPR, HFEA, and ISO requirements. Updates must be approved by Senior Management and communicated to all relevant staff.

LSB record its staff training, and compliance, and the findings of its periodic audits and inspections. Corrective actions where needed are recorded along with cross-checking against DPIAs and SOPs,

Implementation, Review and Revision

This Policy will be reviewed annually and updated as necessary. The LSB Management Team endorses this policy and is fully committed to its implementation. The DPO accepts overall responsibility for this policy and its implementation, management and review.

This policy remains effective until replaced or formally updated. All LSB staff are required to comply with the policy at all times.

Signed by:

DocuSigned by:
jenny fautly
AB591C7EA5584E4...

Jenny Fautly

LSB Data Protection Officer