Information Governance Policy

Last Review Date:	April 2026
Author:	Finance Manager
Approved By:	Board
Approval Date:	April 2026

Contents

1. Introduction and Purpose

The Breastfeeding Network (BfN) is committed to ensuring that personal data we collect, manage and share is handled with the upmost care and integrity. BfN needs to handle personal data in order to provide the best outcomes to everyone who uses our services; using this data is necessary to run our services and manage our resources appropriately.

This Data Protection Policy sets out how BfN manages personal data, in line with all relevant UK data protection laws and regulations.

This policy document provides the strategic framework and high-level commitments that govern BfN's approach to data protection. It is supported by detailed procedures and guidance documents that provide practical implementation instructions for staff and volunteers.

---

2. Scope

This policy applies to **personal data** - any information relating to identified or identifiable living individuals.

What personal data this policy covers

- **Service user information**: names, contact details, health information about breastfeeding support
- **Volunteer and employee personal data**: employment records, contact details, training records
- **Trustee and director information**: declarations of interest, personal details
- **Identifiable information about donors, partners, or contacts**

Who this policy applies to

- All BfN employees
- All volunteers, including peer supporters
- All trustees and directors
- Any contractors, consultants, or temporary workers accessing BfN personal data or systems
- Third-party organisations processing personal data on behalf of BfN

Where this policy applies

This policy covers personal data in all formats (paper, electronic, audio, visual) and applies wherever BfN personal data is stored, processed, or transmitted:

- BfN offices and premises
- Home working environments
- Mobile devices

- Cloud storage and systems
- Email and communication platforms
- Third-party systems used on BfN's behalf

---

3. Policy Statement and Core Principles

BfN is committed to the highest standards of data protection. We recognise that protecting personal data is essential to delivering safe, high-quality services to the families we support, and to maintaining the trust placed in us by service users, volunteers, funders, and partners.

BfN handles all personal data in accordance with seven core principles:

Lawfulness, fairness, and transparency: We process data only when we have a lawful basis to do so, and we are clear and open with individuals about how we use their information.

Purpose limitation: We collect data for specified, explicit, and legitimate purposes, and do not use it in ways that are incompatible with those purposes.

Data minimisation: We collect only the data that is necessary for our purposes, avoiding excessive or irrelevant information collection.

Accuracy: We take reasonable steps to ensure that the data we hold is accurate, complete, and kept up to date, and we correct or delete inaccurate data promptly.

Storage limitation: We retain data only for as long as necessary to fulfil the purposes for which it was collected, in accordance with our retention schedules, and we securely dispose of data that is no longer needed.

Integrity and confidentiality: We protect data against unauthorised or unlawful processing, accidental loss, destruction, or damage through appropriate technical and organisational security measures.

Accountability: We take responsibility for demonstrating compliance with these principles through documentation, training, monitoring, and continuous improvement.

---

4. Roles and Responsibilities

Although every individual within BfN has an obligation to understand and apply this policy, there is a formal governance structure to ensure management and oversight of data protection.

The Board

The board is responsible for ensuring that effective policies and practices are in place in relation to data protection. The board:

- Approves the text of the Data Protection Policy and major changes to related policies
- Ensures appropriate oversight through governance structures

- Appoints the Caldicott Guardian
- Receives reports on data protection compliance and incidents

Caldicott Guardian

Although BfN is not required to have a Caldicott Guardian, the board designates a member with requisite experience as such. Their role is to:

- Ensure continued focus on the protected confidentiality of service-user information at board level
- Ensure appropriate application of the data protection policy throughout BfN
- This appointment is reviewed every three years by the board

Finance, Audit and Risk (FAR) Committee

As data protection is a standing risk to the organisation, FAR plays a vital role in oversight. They:

- Ensure sufficient financial resources are allocated for data protection
- Oversee internal and external audits
- Review items for escalation under the board's risk management strategies
- Escalate items of significant risk to the full board

Chief Executive Officer (CEO)

The CEO is responsible for implementation of the data protection policy. In practice, this implementation is expressly delegated to the Senior Risk Officer(s).

Senior Risk Officer(s)

These officers must:

- Ensure the policy has representative and up-to-date procedures
- Act as representative of data protection matters on the FAR Committee
- Maintain BfN's registration with the Information Commissioner's Office (ICO)
- Ensure timely completion of the NHS's annual Data Security and Protection Toolkit review and Cyber Essentials re-certification
- Lead investigations required under this policy (or delegate where required) and manage remediation efforts
- Report to FAR, the board, the ICO, BfN's insurers and any other impacted party (including service users) as warranted
- Lead training and awareness-raising
- Implement and oversee the procedure for data subject rights
- Maintain BfN's cyber insurance at appropriate levels

Programme Managers

Programme Managers are responsible for:

- Ensuring legally sound data protection requirements in all services they manage
- Promoting a culture of good data protection practice

Staff with management or supervisory oversight

These individuals are responsible for:

- Promoting a culture of good data protection practice
- Ensuring staff and/or volunteers they manage complete appropriate data protection training
- Supporting application of data protection principles and procedures

All BfN staff and volunteers

Every individual must:

- Complete mandatory information governance and cyber essentials training annually
- Recognise when they are using personal data
- Apply this policy and relevant procedures to their work
- Recognise data protection concerns, including potential or actual data breaches
- Report any suspected data breach immediately to their line manager/supervisor
- Handle personal data only in ways necessary for their role
- Keep passwords secure and not share access credentials
- Lock screens when leaving devices unattended
- Only access personal data they have legitimate need to see
- Report any concerns about data protection practices

---

5. Transparency and Privacy Notice

BfN is transparent about how we use personal data. We provide a clear privacy notice that explain:

- What data we collect
- Why we collect it
- How we use it
- Who we share it with
- How long we keep it
- Individual rights

Privacy notices are reviewed regularly and updated when our data processing activities change. Current privacy notices are available on our website.

BfN processes personal data only when we have a lawful basis to do so, typically relying on:

- Consent
- Legitimate interests (including "recognised legitimate interests" introduced by the Data (Use and Access) Act 2025)
- Legal obligation
- Vital interests

For special category data (health information), we rely on additional lawful bases as set out in our privacy notice.

---

6. Individual Rights

BfN respects and facilitates the rights of individuals to:

- **Access their personal data** (subject access requests)
- **Rectify** inaccurate or incomplete data
- **Erase** their data in certain circumstances
- **Restrict or object** to certain processing
- **Data portability** where applicable
- **Withdraw consent** where consent is the lawful basis for processing
- **Make a complaint** about how their data is handled

How we handle data subject rights requests

BfN responds to data subject rights requests in line with the Data (Use and Access) Act 2025. Detailed procedures for exercising these rights, including request forms and the complaints procedure, are maintained separately. Requests should be made to dataandprivacy@breastfeedingnetwork.org.uk

---

7. Information Sharing and Third-Party Management

BfN shares personal data externally only when there is a lawful basis and legitimate reason to do so.

When we share personal data

This may include:

- Sharing anonymised or aggregated data for research, quality improvement, or reporting purposes

- Sharing service user information with healthcare professionals or other services
- Providing information to commissioners, funders, or regulators as required
- Working with IT suppliers, payment processors, or other service providers who process data on our behalf

Working with third parties (data processors)

When working with third parties who process personal data on behalf of BfN, we:

- Conduct appropriate due diligence to ensure they can meet data protection requirements
- Put formal data processing agreements in place that specify security requirements, processing restrictions, and liability arrangements
- Monitor their compliance with agreed standards
- Ensure appropriate arrangements are in place before any processing begins

International transfers

We do not transfer personal data outside the UK without appropriate safeguards. The Data (Use and Access) Act 2025 introduces a new test for international transfers, requiring that the third country's protections are "not materially lower" than UK standards. BfN assesses any international transfers against this standard, acting reasonably and proportionately.

---

8. Data Breaches and Incident Response

Despite our best efforts, data breaches or security incidents may occur. BfN has clear procedures for identifying, reporting, investigating, and responding to such incidents.

What is a data breach?

A personal data breach is any incident that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes:

- Loss or theft of devices or paper records containing personal data
- Unauthorised access to systems or data
- Sending information to the wrong recipient
- Cyber attacks or system compromises
- Accidental disclosure of information

All BfN staff and volunteers must report potential or actual data breaches immediately to their line manager or supervisor who must escalate to the Senior Risk Officer(s) without delay at dataandprivacy@breastfeedingnetwork.org.uk

Do not wait to be certain - if you suspect a breach may have occurred, report it immediately. Early reporting can limit damage.

How we respond

The Senior Risk Officer(s) will:

- Investigate the incident to understand what happened, what data was affected, and what risks result
- Contain the breach and prevent further unauthorised access or disclosure
- Assess whether the breach must be reported to the ICO (required within 72 hours for breaches likely to pose risks to individuals' rights)
- Determine whether affected individuals must be notified
- Report to FAR Committee, the board, and BfN's insurers as appropriate
- Implement remedial actions to prevent recurrence
- Document the breach and response in BfN's breach register

Not all incidents require reporting to the ICO, but all must be documented and reviewed to identify learning opportunities.

---

9. Training and Awareness

Effective data protection depends on everyone understanding their responsibilities. BfN is committed to ensuring all staff and volunteers receive appropriate data protection training.

Mandatory training

Information governance and data protection training is mandatory for all staff and volunteers and must be completed as part of their induction. New starters will be provided with limited, role-appropriate access to BfN systems to enable completion of induction activities. Ongoing or wider access to systems containing personal data is dependent on completion of required training.

Training covers:

- Key data protection principles and legal requirements
- BfN's data protection policy and relevant procedures
- Common risks and how to avoid them
- How to identify and report breaches
- Individual responsibilities
- The internal complaints procedure for data subject rights

Ongoing training

Regular refresher training is provided, typically annually, to ensure continued awareness and to cover any changes to legal requirements, systems, or procedures.

Role-specific training

Individuals with particular data protection responsibilities (Senior Risk Officers, programme managers, those supervising volunteers) receive additional training appropriate to their roles.

Training records

Completion of data protection training is recorded and monitored. Managers and supervisors are responsible for ensuring that those they oversee complete required training.

Awareness-raising

Beyond formal training, BfN promotes good data protection practice through regular communications, sharing learning from incidents or audits, and ensuring that Senior Risk Officers are visible champions of good data protection governance.

The Senior Risk Officer(s) are responsible for the overall training and awareness programme.

---

10. Monitoring, Audit, and Review

BfN monitors compliance with this policy and related procedures through several mechanisms:

Internal monitoring

The Senior Risk Officer(s) conduct regular reviews of data protection practices, including spot checks of records management, access controls, and adherence to procedures. Findings are reported to FAR Committee.

Self-assessment

BfN completes the annual NHS Data Security and Protection Toolkit assessment, which provides a structured review of our data protection practices against national standards.

BfN also maintains certification of Cyber Essentials annually.

External audit

Where required by funders, commissioners, or as part of broader organisational audits, data protection practices may be reviewed by external auditors. FAR Committee has oversight of all audit activity.

Incident analysis

All data breaches and security incidents are investigated and reviewed to identify systemic issues, patterns, or opportunities for improvement. Lessons learned inform updates to procedures and training.

Policy review

This policy is formally reviewed at least annually by the Senior Risk Officer(s) and submitted to the board for approval. Reviews may occur more frequently if:

- Significant legal or regulatory changes occur
- Major incidents reveal policy inadequacies
- Organisational changes affect data protection arrangements
- Good practice guidance indicates improvements are needed

Supporting procedures and guidance documents are reviewed and updated as needed, with material changes reported to FAR Committee. Changes that significantly alter the policy's principles or commitments require board approval.

---

11. Legal and Regulatory Framework

BfN's data protection practices are designed to ensure compliance with all relevant UK data protection laws and regulations.

UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

These establish the comprehensive legal framework for processing personal data in the UK, including requirements for:

- Lawful bases for processing
- Individual rights (access, rectification, erasure, etc.)
- Data protection principles
- Security measures and breach notification
- Accountability and documentation requirements

Data (Use and Access) Act 2025

This Act came into force in June 2025. It introduces targeted amendments to UK GDPR, DPA 2018, and PECR. The Act is being implemented in phases through to June 2026, although several key changes are already in place:

New "recognised legitimate interests" lawful basis for certain types of processing (including safeguarding and emergency response) without requiring a balancing test

Data subject access requests: Clarification that only "reasonable and proportionate" searches are required, and the response deadline may be paused in certain circumstances

International transfers: New data protection test requiring third country protections are "not materially lower" than UK standards (replacing "essentially equivalent")

Mandatory internal complaints procedures for data subject rights requests, with acknowledgement within 30 days

Extended soft opt-in provisions for charity direct marketing communications to individuals who have donated or shown interest

Clarified rules for scientific research and cookies

The Caldicott Principles

As a health-related charity handling sensitive health information about service users, BfN adheres to the Caldicott Principles, which provide a framework for handling confidential patient information appropriately. These principles emphasise:

- Justifying the purpose for using confidential information

- Using confidential information only when absolutely necessary
- Using the minimum necessary confidential information
- Access to confidential information on a strict need-to-know basis
- Everyone's responsibility to understand their obligations
- Compliance with the law
- The duty to share information for individual care

NHS Data Security and Protection Toolkit

BfN completes the annual Data Security and Protection Toolkit to demonstrate our compliance with data security standards expected of organisations handling NHS patient data or providing NHS-funded services.

The Privacy and Electronic Communications Regulations (PECR)

These govern marketing communications (email, text, phone) and the use of cookies and similar technologies on our website.

Compliance and accountability

BfN maintains registration with the Information Commissioner's Office as required under data protection law. We monitor legal and regulatory developments and update our practices accordingly.

Where questions arise about legal interpretation of data protection requirements, BfN seeks advice from the ICO and/or legal advisers specialising in data protection.

---

12. Management of Organisational Records

Whilst this policy focuses on personal data, BfN also maintains organisational records (non-personal information) as part of good governance and legal compliance.

Organisational records we maintain

These include:

- Governance documents (constitution, trustee meeting minutes, strategic plans)
- Financial records (accounts, invoices, contracts, grant agreements)
- Operational records (policies, procedures, service documentation)
- Communications and correspondence of organisational significance

How we manage organisational records

Organisational records are managed according to:

- **Charity Commission requirements** for proper record-keeping and governance
- **Accounting regulations** requiring retention of financial records

- **Contractual obligations** for confidentiality where applicable
- **Good governance practice** to demonstrate accountability and transparency

Retention and security

All organisational records, whether containing personal data or not, are:

- Stored securely with appropriate access controls
- Retained according to our Retention Schedule
- Disposed of securely when no longer needed

Our Retention Schedule specifies retention periods for all types of records.

---

13. Related Documents

This policy is supported by detailed procedures and guidance maintained separately:

Procedures

- Data Subject Rights Procedures (access requests, rectification, erasure, complaints)
- Data Breach Response Procedure
- Privacy Impact Assessment Template
- Data Processing Agreement Template
- Retention Schedule (covering personal data and organisational records)

Templates and Forms

- Privacy Notices (service users, volunteers, employees, website visitors)
- Consent forms
- Data Processing Agreements
- Data Sharing Agreements
- Data Subject Complaints Form

Training Materials

- Information Governance Induction Training
- Information Governance Refresher Training
- Role-specific Training Modules

Guidance

- IT user access policy (passwords, encryption, remote working)
- Safe Data Handling Guidelines for Staff and Volunteers

External Resources

- ICO guidance (ico.org.uk) including guidance on the Data (Use and Access) Act 2025
- NHS Data Security and Protection Toolkit (dsptoolkit.nhs.uk)
- Caldicott Principles guidance
- Cyber Essentials scheme (ncsc.gov.uk)
- Charity Commission guidance on record-keeping

All related documents and procedures are accessible to staff and volunteers through SharePoint: Shared Files – for general use, Policies and Procedures, Information Governance.

Questions about this policy should be directed to the Senior Risk Officer(s) at dataandprivacy@breastfeedingnetwork.org.uk

---

14. Key Definitions

Caldicott Guardian: A senior role responsible for protecting the confidentiality of service user information.

Consent: Freely given, specific, informed, and unambiguous agreement by an individual to processing of their personal data.

Data breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Data controller: The organisation that determines the purposes and means of processing personal data. BfN is the data controller for most data it holds.

Data processor: An organisation that processes personal data on behalf of a data controller. Examples include IT service providers or payment processors used by BfN.

Data subject: An individual whose personal data is processed.

Personal data: Information relating to an identified or identifiable living individual.

Processing: Any operation performed on personal data, including collection, recording, storage, retrieval, use, disclosure, erasure, or destruction.

Recognised legitimate interests: A new lawful basis for processing introduced by the Data (Use and Access) Act 2025 for specific purposes that does not require a balancing test

Special category data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation.