Information Governance Policy

Date of Issue:	August 2023	**Next Review Date:**	August 2024
Version:	2	**Last Review Date:**	June 2022
Author:		Central Support Manager, Clare Farquhar	
Approval Route			
Approved By:		**Date Approved:**	
FAR Committee			
Links or overlaps with other strategies/policies:			
IT Policy			
BfN guidelines for running video (Zoom) calls			
Information Governance Annual Audit and Improvement Plan			
Privacy Policy			
Social Media Policy			
Code of Conduct			
Records Retention Policy			

Contents

1. Introduction

Information Governance ("IG") allows the Breastfeeding Network and individual members of staff and volunteers to ensure that information, including personal and sensitive information, is obtained fairly and lawfully, held securely and confidentially, recorded accurately and reliably, used efficiently and ethically and shared appropriately and legally, in order to give the best possible care to breastfeeding women and their families.

1.1 Why does BfN need information?

BfN needs information to provide the best service to breastfeeding mothers and those who care for them and to manage services and resources.

We must manage information securely, efficiently and effectively; suitable policies, procedures and management accountability are required to create a solid governance framework for information management. Good information management is also important for:

- Building and maintaining trust
- Keeping within the law
- Meeting the requirements of our contracts and funding arrangements

2. Scope of the Document

IG covers all types of information about volunteers, employees and service users and the organisation. Everyone in BfN is responsible for it.

3. Policy statement

The policy sets out information handling standards and describes the tools BfN will use to achieve these standards to develop a consistent approach to handling personal and organisational information. This will lead to improvements in information handling activities and ensure service user confidence in the Breastfeeding Network.

4. Aim of this Policy

The purpose of this policy is to provide a statement on the use and management of information within BfN and describe the arrangements for providing assurance to the Board that IG standards are defined and met and IG incidents appropriately managed. This will enable us:

- To promote the effective and appropriate use and sharing of information.
- To understand our performance and manage improvements in a systematic and effective way to meet the Information Governance Assurance requirements set out by the Chief Executive of the NHS.
- To encourage joint working between the Breastfeeding Network, the NHS and others, preventing duplication of effort and enabling more efficient use of resources.

4.1 Objectives

- To ensure that personal data on service users, volunteers and employees is handled securely and legally by all BfN volunteers and employees.
- To provide a framework to bring together all the requirements, standards and best practice that apply to the handling of personal information.
- To establish guidelines to ensure information is accurately recorded and to ensure it is accessible when needed.
- To monitor progress against agreed standards and plan improvements.
- To establish a procedure for managing IG incidents.
- To establish a procedure for handling Subject Access requests.

5. Internal IG Governance (Bodies and Structure) and Responsibilities

5.1 BfN Board of Directors

The role of the Board is to define the BfN policy in respect of Information Governance, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Board receives the Information Governance Audit Report and Improvement Plan on an annual basis. Regular reporting to the Board will be through the Finance Audit and Risk (FAR) committee.

5.2 Caldicott Guardian
All NHS organisations must have a Caldicott Guardian. As a matter of good practice, BfN appoints a Board member as Caldicott Guardian with responsibility for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The duties and responsibilities of BfN's Caldicott Guardian are outlined here The Caldicott Principles - GOV.UK (www.gov.uk)

Acting as the 'conscience' of an organisation, the Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board level and, where appropriate, at a range of levels within the organisation's overall governance framework.

5.3 Finance, Audit and Risk Committee (FAR)
FAR meets on at least a quarterly basis. Its objectives include ensuring effective internal audit functions are in place and ensuring policies are up-to-date and fit for purpose. IG is a regular item on the FAR agenda.

FAR will:

- Ensure that IG policies are in place and subject to regular review;
- Review the biennial audit of IG practices carried out by the central team;
- Scrutinise the annual IG audit and improvement plans; and
- Receive reports on all major IG incidents.

5.4 Chief Executive Officer (CEO)
The CEO oversees the development and implementation of the Information Governance policy with express delegated responsibility to the Finance Manager.

5.5 Finance Manager
The Finance Manager is the Senior Information Risk Officer (SIRO) for BfN. The Finance Manager:

- Is familiar with and takes ownership of BfN's information governance policy;
- Acts as a representative of IG matters on the FAR Committee;
- Maintains BfN's registration with the Information Commissioners Office and ensures completion of the annual IG audit which demonstrates our commitment to the protection of personal information and to the improvement of our processes in line with any updates or changes in legislation.

5.6 Programme Managers
The Programme Managers are responsible for ensuring IG policy compliance within each local peer support service. Regular audits will be carried out to measure compliance and identify any areas for improvement.

5.7 Service Coordinators/Line Managers/Supervisors
All Service Coordinators, Line Managers and Supervisors within BfN are responsible for ensuring that all members of staff and volunteers have completed relevant IG training modules and are complying with agreed policies and procedures on a day-to-day basis. Refresher training should be completed on an annual basis and recorded on the individual training log and annual appraisal.

5.8 Staff and volunteers
The majority of BfN staff and volunteers handle information in one form or another. Staff and volunteers who in the course of their work create, use or otherwise process information have a duty keep up to date with and adhere to relevant legislation, case law and national guidance. BfN policies and procedures listed above will reflect such guidance and compliance with these policies will ensure a high standard of IG compliance within BfN.

BfN has a legal obligation to maintain the confidentiality of the personal information it processes and must do so to maintain the trust and confidence of those who use our services. Breaches of confidentiality may be treated as serious disciplinary incidents which in some circumstances can lead to dismissal. All staff should ensure they are aware of the relevant BfN policy in respect of any personal information they may process.

5.9 Training and Guidance

Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. The following approach ensures that all staff receive training appropriate to their roles. All staff will:

- be briefed on IG requirements as part of their induction;
- Receive further training and annual updates as required; and
- Understand and comply with the IG policy

5.10 IG Awareness

To ensure that raising awareness of and compliance with information governance standards is raised, information will be disseminated via:

- Internal communications;
- Staff meetings, including 1-1's and staff appraisals; and
- Formal and informal training.

5.11 IG Internal Reporting

Day to day IG issues should, in first instance, communicated to a member of the Central Staff Team, a list of whom can be found on our website or, for staff working within a peer support service, to the Programme Manager. IG issues will then be tracked by the Programme Managers working with the IG Lead, assessed by key central staff and recorded via the project toolkit. These issues should be reviewed on a monthly basis.

The SIRO (Finance Manager) will report any operational IG issues, risks or policy developments to the FAR (Finance, Audit and Risk Committee) every two months as part of the regular agenda.

The procedure for reporting and investigating any suspected breaches of the IG policy is detailed within this document. A central log of all incidents is maintained and reported periodically to the Board.

The SIRO, Central Management Team and local IG leads (Service Coordinators) will:

- Develop an audit tool to assess BfN's compliance with its IG policies, in peer support services, in the central team and by volunteers out-with projects by local supervisors
- Review the audit tool on a regular basis to ensure it is relevant and in line with best practice
- Conduct an audit of IG practices every two years
- Will advise on any local or central changes in procedure (collection of new data or changes in data storage practice)
- Record all IG incidents
- Report serious or urgent IG incidents to FAR (for onward reporting to the Board where considered appropriate) as they occur and consult as required on any actions needed
- Analyse, investigate and upward report of incidents and any recommendations for remedial action
- Report to the board on annual IG audit and improvement plans
- Communicate IG developments and standards to appropriate volunteers and staff

6 Relevant articles of law

6.1.1 Data Protection Act (2018)

According to Data protection - GOV.UK (www.gov.uk) "The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.
The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary

- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation
- There are separate safeguards for personal data relating to criminal convictions and offences.

6.1.2 Individual rights

Under the Data Protection Act 2018, individuals have the right to find out what information the government and other organisations store about them. These include the right to:

- be informed about how their data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of their data
- data portability (allowing individuals to get and reuse their data for different services)
- object to how their data is processed in certain circumstances

Individuals also have rights when an organisation is using their personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests"

6.2 The UK GDPR

The UK General Data Protection Regulation (UK GDPR) currently applies to all organisations in the UK which process personal information. Breaches of the UK GDPR may be investigated by the Information Commissioner's Office and a penalty of up to £17.5million or 4% of annual turnover can be awarded.

Multiple areas of the UK GDPR apply to BfN's work and it is important that each understand your responsibilities.

7 Definitions

7.1.1 Personal Data

According to the Information Commissioner's Office, the following definition applies:

- "The UK GDPR applies to the processing of personal data that is:
    - wholly or partly by automated means; or
    - the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
    - can be identified or who are identifiable, directly from the information in question; or
    - who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised then the anonymised data is not subject to the UK GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data."

7.1.2 Children

Recital 38 of the UK GDPR states that:

"Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

We may rely on any of the bases given in Article 6 as our lawful basis for processing a child's personal data. However, for some of the bases there are some important additional considerations that we need to take into account when the data subject is a child.

Any processing of data relating to children should be reviewed to ensure that it is fully compliant with the UK GDPR requirements.

7.1.3 Processing

The UK GDPR regulates the "processing" of personal data.
Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including
(a) Organisation, adaptation or alteration of the information or data,
(b) Retrieval, consultation or use of the information or data,
(c) Disclosure of the information or data by transmission, dissemination or otherwise making available,
or
(d) Alignment, combination, blocking, erasure or destruction of the information or data.

The UK GDPR requires that our lawful basis for processing must be clearly identified. The three bases that apply to BfN are consent, contract and legitimate interest. (see Privacy Notice)

7.1.4 Data Subject

Data subject means an individual who is the subject of personal data.
In other words, the data subject is the individual whom particular personal data is about. The UK GDPR does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

7.1.5 Data Controller

Data controller means: a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
A data controller must be a "person" recognised in law, that is to say:

- individuals;
- organisations; and
- other corporate and unincorporated bodies of persons.

For some of the information we hold. BfN will be the data controller. In other areas, particularly commissioned services, BfN will be defined as either joint controller or data processor. This is important to note and should be

clearly defined within the service level agreement, data sharing agreement or contract. Where BfN is the data controller or joint controller, the nominated contact for any queries or issues is the SIRO.

8 How is data processed?

Information about how data is processed by BfN is given in the Privacy Notice on our website http://www.breastfeedingnetwork.org.uk/privacy-notice/. This should be stated clearly on any forms collecting personal data or requesting consent to process personal data, including paper and online forms. In any situations where BfN is not the data controller, or is joint data controller, the relevant privacy notice information should also be provided to service users.

Anonymised records, such as Call record sheets or BfN Breastfeeding Centre monthly record sheets, can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym or collection of facts about a service user that may identify them to a particular individual. This means that taking steps to fully anonymise information wherever possible is very important as it enables information to be processed while reducing any risk to the individual or BfN.

9 Your responsibilities when you process data

Under the UK GDPR, BfN is required to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. Data protection should be integrated into all data processing activities at every stage (data protection by design and by default). This can be achieved by discussing data processes with the Finance Manager and Caldicott Guardian, if required. A Data Protection Impact Assessment may be required if processing is likely to result in high risk to individuals. A template is available in Shared files for general use in SharePoint. Your Programme Manager or the Finance Manager can also provide examples of those that have previously been completed. A suggested patient data protocol is also shown in Appendix 3.

Wherever possible, we should have the consent of any parent or volunteer before we process any information about them. Explicit consent means clear, voluntary, freely given indication of preference or choice, where our privacy information has been made clear. Consent should ideally be given in writing using an agreed consent form. If this is not possible or practical, verbal consent can be accepted but it should be noted on contact sheet by the person requesting consent when and to whom this was given. Where consent is not practical, we can look at "legitimate interests" or "contract" as our legal basis for processing personal information.

10. Confidentiality and Data Protection Assurance

10.1 Caldicott Principles

There are eight Caldicott Principles that provide guidance when handling client information. These are questions that you should ask yourself before processing or disclosing personal information:

1. Justify the purpose(s) of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality
8. Inform patients and services users about how their confidential information is used

Additional information to help us maintain a confidential service is available from the 'Code of practice on confidential information" at: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care .

11. Online services and social media support

BfN has issued clear guidance on the protection of privacy, confidentiality and the security during any type of online video call. The IT policy should also be followed by anyone delivering this type of support to parents, staff or volunteers to minimise the risk of security breaches. All the usual principles of consent apply (e.g. before adding members to a group, before taking photos of the group etc.) and extra precautions are required due to the increased risk of working online.

12. Information Security Assurance

This section covers both manual and electronic records to safeguard information from being disclosed inappropriately, either by accident or design, whilst it is being transferred or communicated within and outside of BfN.

The BfN IT policy outlines all the steps which must be taken to ensure the security and confidentiality of any information held electronically.

BfN will maintain an information asset register for its information, software, hardware, and services which includes the owner and location of each asset and audit all equipment, static and portable.

Non-computerised records systems should also have an asset register containing relevant file identifications and storage locations.

Risk assessments should be carried out by anyone responsible for processing personal data to identify potential information security incidents, particularly those that could adversely affect business continuity, measures should then be put in place to either remove or reduce the risk.

Volunteers and employees must not leave portable computers, client's notes or files in unattended cars or in easily accessible areas. All files and portable equipment should be stored under lock and key when not actually being used and overnight. Mothers records, if taken home, should be stored securely to prevent anyone else having access to the notes, procedures for safeguarding the information effectively should be locally agreed.

If employees or volunteers are required to carry any device or folder containing personal or confidential information whilst travelling then all reasonable steps must be taken to ensure the security of that information such as not leaving laptops or bags unattended, locking bags or laptops to a rail or table-leg if possible and taking extra care not to leave anything behind.

12.1 Mobile Phones

The BfN IT policy outlines the requirements of any device accessing BfN systems, including smartphones. In addition, any member of staff or volunteer who is issued with a mobile phone belonging to the BfN must comply with the following:

The phone remains the property of BfN. It should not be changed or altered in any way without authorisation. It should be returned immediately if you no longer require it for work, or if you terminate your employment with BfN.

1. The phone should only be used for reasonable work or volunteering related purposes
2. Any loss, damages or faults must be reported immediately to your Line Manager
3. All entries (contacts etc.) must be saved to the SIM card and not to the mobile phone memory.
4. The phone should be protected by a PIN number or suitable alternative security measure to prevent unauthorised access
5. You should make every effort to keep the phone safe. Keep it with you whilst on duty, even if turned off. You should not leave it on view in your car or on your desk.
6. BfN will not be liable for any fines or endorsements given to staff who disregard the mobile phone rules.
7. Remember that mobile phone numbers can be traced or displayed on phones with caller I.D.
8. For confidentiality purposes, when returning a mobile phone, SIM cards/phone memory must be cleared of text/voice messages and personal phone numbers.

Any information relating to BfN activities held on a personal mobile phone must be covered by the same security measures outlined above.

12.2 Keeping information to a good standard

We can all help maintain BfN's reputation by being careful with emails we send – double check the addressee and pause before you hit the send button - and check you would be happy to sign your name to if it was a letter being published in the newspapers.

All BfN emails should be sent with a standard footer using BfN branding explaining to the recipient that you are from the Breastfeeding Network and containing link to our Disclaimer as shown in Appendix 2.

13. Records Management

BfN will continue to develop and improve good record systems based on the Nursing and Midwifery Council code: Professional standards and behaviour for nurses and midwives as an example of best practice https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf

We will also refer to the Records Management Code of Practice https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care

BfN works in partnership with providers and commissioners of services and BfN members will be expected to be orientated to local documentation policies. BfN workers will be expected to record support given using the principles outlined in the NMC Code.

BfN, in line with NHS guidance, has a policy for the suitable retention and timely disposal of records (see Appendix 4). Records relating to breastfeeding support will be recorded in the Personal Child Health Record book (Red Book) or maternity notes, with agreement from parents and/or health professionals. In areas with funded peer support programmes, it may be necessary to have separate records describing the information and support given to mothers.

BfN's record retention policy applies to both paper and electronic records and there should be a systematic procedure in place for the review of these records. Personal information will be destroyed under confidential conditions (securely shredded).

Improving the quality of the information we hold is the key to improving the service we give to family's babies. If you have a computer account, you will be responsible for maintaining effective document management system within it, preventing unauthorised access with inherent potential for data corruption or loss and for backing up the data regularly.

14. Information Sharing

By setting standards for the effective and appropriate handling of information this Information Governance policy will help us to work with other organisations, share good practice ideas and avoid duplication through shared efforts.

15. Information Governance– annual assessment of compliance

Data Security and Protection Standards for health and care sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

BfN is required to undertake an annual IG assessment using the NHS Digital Data Security and Protection toolkit https://www.dsptoolkit.nhs.uk/.

IG assessments need to be submitted annually by 30 June each year to demonstrate standards are being improved or maintained, and will if necessary, need to be supported by action/implementation plans.

The key requirements defined within the NHS Operating Framework are also the key requirements necessary for the IG assessment.

The assessment process requires the development of an implementation plan which requires that regular audits are carried out across BfN, both centrally and in local peer support services.

16. Training

All staff and volunteers are required to complete the relevant modules using the NHS Digital e-learning tool NHSE elfh Hub (e-lfh.org.uk) (available via www.bfntraining.org.uk) and to undertake updates on an annual basis.

The relevant modules are as follows:

Course	Who
Data security awareness for volunteers	Helpers, Helpline Supporters, paid and voluntary
Data security awareness Level 1	Supporters, Central staff, administrators, Service Coordinators, Volunteer Coordinators, Tutors, Supervisors

17 Procedure for reporting and managing a potential breach of the UK GDPR and/or the Common Law of Confidentiality

17.1 What is a breach?

According to The Information Commissioners Office a breach is defined as: "A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed."

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data

17.2 What to do if you think a breach may have occurred

If anyone believes that an IG incident has occurred the first step is to report this to your Line Manager or Supervisor who should then report to the Finance Manager. If it is not possible or appropriate to go via a Line Manager then the next point of contact is the Finance Manager directly (contact details on our website). The Line Manager or the Finance Manager will need to know the circumstances of the potential incident so please provide as much detail as possible.

The following steps should then be taken in consultation with the Finance Manager:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation. This should be done immediately if you suspect there has been a breach. You should then inform your Line Manager or the Finance Manager of the steps you have taken to retrieve lost information or to minimise the risk of misuse such as:

    - Retracing your steps to see if you can find missing files or devices
    - If you have lost a mobile phone contact the provider and ask them to block access to the SIM
    - Change your passwords on any email accounts, social media sites, SharePoint or anything else that could be accessed via your laptop of tablet

2. Assessing the risks – you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen. Support will be given by the Finance Manager and if necessary by our Caldicott Guardian to assess the level of risk and to determine who is the data controller in each individual case. If the level of risk is potentially

high, and if we consider that BfN is the data controller, then the IG Incident Reporting Tool via the IG Toolkit https://www.igt.hscic.gov.uk/ will be used to officially record the incident and follow-up actions. This should be updated within 24 hours of BfN becoming aware of a Serious Incident Requiring Investigation (SIRI).

3. Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. You should be clear about who needs to be notified and why. You should, for example, consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media. Any breaches notifiable to the ICO must be reported within 72 hours of the incident. Guidance on assessing whether or not an incident is reportable can be found here UK GDPR data breach reporting (DPA 2018) | ICO. If BfN is considered to be the data controller this step should be handled by BfN with the support of the Finance Manager and Caldicott Guardian. If a third party is considered to be the data controller then that third party should be notified of the incident, with all the supporting information detailing why we consider them to be the data controller. It is then up to the third party to take further steps relating to investigation and reporting.

4. Evaluation and response – it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly. This should be done in all cases, whether BfN is the data controller or not. Relevant procedures should be reviewed and updated to prevent recurrence of the incident that occurred. The outcome should be reported to and agreed by the Finance Manager and Caldicott Guardian.

18 Subject Access Requests

Under the UK GDPR individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request or 'SAR'.

Requests should be made in writing to the Paisley office or by email to admin@breastfeedingnetwork.org.uk. Requests can also be made by telephone by calling the Paisley office. If possible, we will ask the individual to specify the information or processing activities that their request relates to, if it is not clear. The timescale for responding to the request will be paused until clarification is received.

BfN will also ask for ID to confirm the identity of the requestor. The timescale for responding to a SAR does not begin until the requested information has been received, however ID documents should be requested promptly.

The information will be provided in writing, electronically or verbally as preferred by the requestor.

Individuals who make a request are entitled to be:

a. told whether any personal data is being processed;
b. given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
c. given a copy of the information comprising the data; and given details of the source of the data (where available).
d. Provided with other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

All Subject Access requests will be dealt with promptly and wherever possible within 30 days of receiving it. The timescale may be extended by a further two months if the request is complex. Information will be provided free of charge, except where a request is considered to be manifestly unfounded or excessive, particularly if it is repetitive, in which case a "reasonable fee" may be payable.

APPENDIX 1
Related Links and Information

Our organisation must comply with the guidance and legislation from the sources below:

- The General Data Protection Regulation https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- The Data Protecion Act (2018) Data protection - GOV.UK (www.gov.uk)
- Health and Social Care Act 2012 http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted
- The Human Rights Act 1998 http://www.legislation.gov.uk/ukpga/1998/42/contents
- BfN Code of Conduct
- UK Caldicott Guardian Council https://www.gov.uk/government/groups/uk-caldicott-guardian-council
- The Common Law duty of confidentiality http://webarchive.nationalarchives.gov.uk/+/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_5803173

Breastfeeding Network is a Registration number Z2041090 registered Data Controller Security number 10821264
The Information Commissioner's Office http://www.ico.gov.uk/
Information Governance Toolkit Organisation Search (dsptoolkit.nhs.uk)

What you should know about Information Governance
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance
Caldicott guidelines The Caldicott Principles - GOV.UK (www.gov.uk)
Freedom of Information Act http://ico.org.uk/for-organisations/guide-to-freedom-of-information/
BfN is not included within FOI requirements.

APPENDIX 2
Standard Email Footer and Disclaimer

Name
Job Title
Standard working days and times

The Breastfeeding Network aims to be an independent source of support and information for breastfeeding women and for those involved in their care.
To talk to a mum who knows about breastfeeding call the National Breastfeeding Helpline 0300 100 0212.
The Breastfeeding Network, PO Box 11126, Paisley PA2 8YB www.breastfeedingnetwork.org.uk
Disclaimer **http://www.breastfeedingnetwork.org.uk/email-disclaimer/**
The Breastfeeding Network is a Registered Charity No SC027007.
The Breastfeeding Network is a Company Limited by Guarantee Registered in Scotland. Company No. 330639
Registered Office: Whitelaw Wells, 9 Ainslie Place, Edinburgh, EH3 6AT
Save paper: please think before you print this email.

APPENDIX 3

PATIENT INFORMATION PROTOCOL OFFICE COPY

1. Patient gives consent to being contacted by BfN (include consent to use anonymised non-personal data to evaluate the service)
2. Hospital staff will collect names and addresses of women who want to join the service and assign each mum a unique ID
3. Hospital staff phone unique ID, names and phone numbers only to Community Coordinators
4. Hospital staff will post the paper forms with personal details to the administrator to enter onto a database (registered post) or will enter the details onto the database directly
5. Community coordinators will ring mums and get addresses again if they need to do home visits.
6. Peer Supporter keeps all patient information securely on paper (only those details necessary to provide service)
7. Peer Supporter phones patient, and gets address from patient only if a visit is required
8. If peer supporters need to pass information between them when supporting a mum, they would use the phone or only initials/unique IDs in an email
9. When a mum finishes the service all paper records will be sent to the administrator to enter onto the database, by Registered Post
10. Peer Supporter destroys notes at an agreed point
11. All paper records at all stages will be kept in locked boxes for security.
12. Administrator enters data from hospital and community onto spreadsheet/database, using unique ID. Do not store personal data e.g. name and address.
13. Administrator's laptop to be kept in a locked cupboard when not in use, and backed up weekly.

- Forms used to record patient details need to be approved by Caldicott Guardian.
- All paper records at all stages kept in locked boxes for security
- Only data needed to provide service to be collected and kept
- Data to be destroyed once service ended in line with Records Retention Policy
- Evaluation data stored using ID, not personal identifying data

Project Name.....Project Manager.....

I confirm that all staff working on this project will work within the protocol detailed above.
Signed..... Date.....

Information Commissioners Office (ICO) – POWERS TO FINE UP TO £17.5million OR 4% OF ANNUAL TURNOVER PER BREACH AND IMPOSE CUSTODIAL SENTENCES

Appendix 4
Records Retention Policy

BfN has developed a records retention policy to ensure compliance with Article 5e of the GDPR – personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. It will also ensure that all types of records are kept for an appropriate amount of time. This is based on the NHS Code of Practice, the CIPD checklist of retention periods and HMRC Minimum retention periods for manual records.

This is a summary of the retention period for each type of record. Records (whatever the media) may be retained for longer than the retention period if there is a good reason for this (e.g. a business need). However, records containing personal data should not generally be kept any longer than the retention period. In all cases, records should be destroyed securely and a log of destruction should be maintained.

If a record falls into more than one category, then the longer retention period should apply. If these guidelines differ from the requirements of a local commissioner or funder, then a request should be made in writing/email to the relevant Programme Manager for consideration and approval by the central IG team.

The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound):

- records relating to individual support
- administrative records (including personnel, financial and accounting)
- records, and notes associated with complaint handling;
- photographs, slides and other images (clinical & non-clinic);
- audio and video tapes, cassettes, CD-ROMs, etc.
- e-mails;
- computerised records; and
- scanned documents

Any details of breastfeeding support should ideally be recorded in the Personal Child Health Record book (Red Book) or maternity notes. For record retention purposes this ensures the records will be kept for the appropriate time. Where this is not feasible, all efforts must be taken to anonymise the records as much as possible and to ensure a secure method of transfer and storage.

For further details see this link https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care

Please note that many of these records will be held at the Paisley office and therefore once they have been processed it may not be necessary to keep duplicate copies locally. Likewise, if information is transferred from paper to electronic records you should consider whether or not it is appropriate to keep the information in duplicate forms.

Any requests for changes to the retention schedule (such as the addition of new types of record or the amendment of a retention period) should be made in writing/email to the central IG team. The Finance Manager will decide whether any changes are necessary.

Type of record
Minimum retention period

Type of record	Minimum retention period
Support records	
Records containing personal data or sensitive personal data– such as referral forms, drop-in data, feedback/evaluation forms	2 years
Contact sheets detailing the support given, topics discussed, specific concerns	8 years
Contact details for the purpose of gathering feedback (email addresses or telephone numbers)	4 months
Anonymised feedback forms where data has been transferred to a computerised system or report	6 months from data entry or date of report
Text messages	3 months
Web chats/social media messages	6 months
Diaries	2 years after end of year to which diary relates.
Training enquiries	2 years
Administrative records	
General email messages	6 months – attachments and emails should be saved as files rather than saved in the email account
All accounting records inc. daybooks, ledgers, cashbooks, stock records, expenses records, purchase invoices, sales orders, sales invoices, credit notes, debit notes, receipts, transactions, cheques, paying in books, bank statements, VAT records	6 years
Audit reports – internal and external (including management letters, value for money reports and system/final accounts memoranda)	2 years after formal completion by statutory auditor
Annual audited accounts and organisational records including Board minutes and agendas	Permanently
Copies of purchase orders or delivery notes	1 year
Funding agreements/SLAs	6 years
Procurement requests/quotations	2 years
Business plans	Permanently
Operational reports	6 years
Meetings and minutes papers (other, including reference copies of major committees)	6 years
Incident records – e.g. breaches of IG or Safeguarding policy, health and safety incidents,	10 years
Complaints	10 years from completion of action
Serious incident files - events where the potential for learning or the consequences are so significant, that they warrant a comprehensive response e.g. serious breaches of IG or safeguarding policies	20 years
Patient information leaflets	10 years after the leaflet has been superseded
Subject access requests – records of requests	3 years after last action
PAYE, payroll, NI, income tax records and correspondence with HMRC	10 years after the end of the financial year
Recruitment records (successful)	3 years following termination of employment
Recruitment records (unsuccessful candidates)	1 year
Staff/volunteer records –personal files, letters of appointment, contracts, references, training records, equal opportunity monitoring forms, timesheets, leave/absence records, disciplinary/grievance records	6 years after the individual has left