Information Governance Policy

Date of Issue:	May 2018	**Next Review Date:**	May 2020
Version:	2	**Last Review Date:**	February 2016
Author:		Central Support Manager, Clare Farquhar	
Approval Route			
Approved By:		**Date Approved:**	
Links or overlaps with other strategies/policies:			
Information Governance Management Framework			
Information Governance Annual Audit and Improvement Plan			
Privacy Policy			
Social Media Policy			
Records Guarantee			
Code of Conduct			
Records Retention Policy (Appendix 4)			

CONTENTS

Appendices

1. Introduction

Information Governance 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; so we need suitable policies, procedures and management accountability 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

Information Governance covers all types of information about volunteers, employees and service users but it also covers information about the organisation and 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 improve 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 and the NHS, 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. Responsibilities

BfN Board of Directors

The Boards' role 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.
They will receive 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.

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 http://scot-ship-toolkit.org.uk/roles-and-responsibilities/caldicott-guardians

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.

CEO

The Chief Executive oversees the development and implementation of the Information Governance policy with express delegated responsibility to the Central Support Manager.

Central Support Manager

The Central Support Manager is the Senior Information Risk Officer (SIRO) for BfN. The Central Support 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.

Programme Managers

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

Project Leads/Line Managers/Supervisors

All Project Leads, 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.

All 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 Information Governance 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.

6. Defining Different Types of Information and how it is handled

6.1 Definitions

Information can be classified in a number of different ways:

6.1.1 Personal Data

According to the Information Commissioners Office, "The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual."

Information about individuals is considered personal when it enables an individual to be identified. For example contact record sheets or trainee/staff records

6.1.2 Sensitive Personal Data

The GDPR refers to sensitive personal data as "special categories of personal data" and includes:-

(a) The racial or ethnic origin of the data subject,

(b) Her political opinions,

(c) Her religious or philosophical beliefs or other beliefs of a similar nature,

(d) Whether she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) Any genetic or biometric data held solely for the purpose of uniquely identifying a natural person

(f) Her physical or mental health or condition,

(g) Her sexual life,

(h) The commission or alleged commission by her of any offence, or

(i) Any proceedings for any offence committed or alleged to have been committed by her, the disposal of such proceedings or the sentence of any court in such proceedings.

6.1.3 Processing

The 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 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 Appendix 3)

6.1.4 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 Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

6.1.5 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.

6.1.6 Person based but anonymised information

For example, Call record sheets or BfN Breastfeeding Centre monthly record sheets, can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym 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 mum or BfN.

6.1.7 Documents

That are not about individuals, for example BfN accounts are not considered personal information but may be classed as confidential. This could be, for example, for commercial reasons or because they contain legal advice. They may also be regarded as sensitive in a general sense because of their subject matter.

6.2 General Data Protection Regulation 2016

The General Data Protection Regulation (GDPR) 2016 applies to all organisations in the UK which process personal information. Breaches of the GDPR may be investigated by the Information Commissioner's Office and a penalty of up to 20 million Euros or 4% of annual turnover can be awarded.

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Ideally we should have the consent of mothers before we process any information about her. 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. If this is not possible or practical, verbal consent can be accepted but it should be noted 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.

Further details are given in Appendix 3.

6.3 What sort of Information does BfN hold?

- Information about people who we support (these might be mothers at drop-ins or in hospital, those who phone the National Breastfeeding Helpline, those who email, those who contact us via online chat, those who contact us via social media, those who contact us by text, those who have been referred to one of our peer support services and those who sign up to receive support from us)
- Staff details
- Information about people who have applied to work or volunteer with us
- Information about our trainees and volunteers
- Information about members of our Friends schemes
- Information about our Directors
- Information about next of kin/emergency contacts

- Information about referees
- Photographs of staff, volunteers, mothers and babies
- Information about people who donate or fundraise for us
- Information about our Commissioners and people who work for them
- Information about shop customers, online, post and by email
- Information about people who speak at our events
- Information about our suppliers
- Information about people who enquire about training with us
- Information about people who respond to our surveys or questionnaires
- Information about people who visit our website
- Information about people who email us to make an enquiry, report a concern or complaint or give us feedback
- Financial and strategic information about the organisation

6.4 What form will this information be in?

- Paper records such as letters, forms
- Electronic files on computers, phones, mobile storage devices, laptops, and tablets
- Databases/spreadsheets
- Emails
- On SharePoint or OneDrive
- On our website
- In our newsletter
- Cloud-based systems or financial system, such as training sites, payroll systems, OCN and Sage

6.5 Where will this information be held?

- In the Paisley office
- In local project offices
- At Drop-Ins, Children's' Centres and other health service premises such as hospitals
- In staff/volunteers' homes
- In electronic or virtual cloud storage systems such as Office 365 (all data servers are based within the EEA or adequately protected e.g. EU US Privacy Shield)
- At the auditors' premises

7. Confidentiality and Data Protection Assurance

7.1 Caldicott Information Management Principles

There are six Caldicott Information Management 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

Additional information to help us maintain a confidential service is available from the 'Code of practice on confidential information"; 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.

It also includes training for relevant people within the organisation and the development of systems to enable possible breaches or risk of breaches to be identified and rectified with confidentiality audits to discover whether any possible breaches occurred through deliberate misuse of systems, or of poor controls. Confidentiality audits include both electronic records management systems and paper record systems.

8. 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.

8.1 Equipment and BYOD (Bring Your Own Device)

Ideally all records should be held or accessed using equipment purchased by BfN.

Employees or volunteers who need to use their personally-owned IT equipment for BfN purposes (including PCs, laptops, tablets and smartphones):

- Must be explicitly authorised to do so by their Line Manager,
- Must secure organisational data to the same extent as on BfN-owned IT equipment
- Must not introduce unacceptable risks (such as malware) onto BfN networks (SharePoint) or to colleagues via email by failing to secure their own equipment.
- Must maintain a clear separation between the personal data processed on behalf of BfN and that processed for the device owner's own purposes, for example, by having different user names for work and personal use.
- BYOD users must use appropriate forms of user authentication such as user IDs and passwords
- Must take all reasonable steps to prevent loss or unauthorised access to sensitive personal information or confidential information

- BfN has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete the data as required.
- BfN has the right to seize and forensically examine any device believed to contain, or to have contained, organisational data where necessary for investigatory or control purposes.

While employees have a reasonable expectation of privacy over their personal information on their own equipment, the organisation's right to control its data and manage devices may occasionally result in support staff unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, BYOD users are advised to keep their personal data separate from business data on the BYOD using different user names

8.2 All equipment

The following rules apply to any equipment used to support the work of the BfN:

- Suitable antivirus software must be properly installed and running on all devices
- Users must ensure that valuable organisational data created or modified is backed up regularly, preferably onto a BfN SharePoint site.
- Any device used to access, store or process sensitive personal information must encrypt data or store files in an encrypted section of the hard drive.
- Personal data must not be held on portable media (including laptops, mobile phones, memory sticks or tablets), unless there is a definite need to do so and this has been approved by the Central Support Manager.
- Personal data must not be sent via unencrypted email or unregistered mail.
- All portable media used by BfN should be logged by the Central Support Manager to track its use and location.
- Where personal information is held on portable media it will be encrypted or held within an encrypted section of the hard drive.
- A password-protected screensaver should be used to prevent unauthorised access to electronic data. This should be launched automatically if the device is inactive for more than five minutes.
- Passwords should be at least six characters long with a mixture of letters, upper and lower cases, numbers and symbols.
- Where general access to rooms is unrestricted, it is good practice to clear desks of all personal and confidential information if the rooms are left unattended for any length of time and to ensure that such information is locked securely away overnight.
- If you are using a BfN laptop for any non-work related emails or documents, e.g. private emails, these should be stored in your email account or network folder clearly marked as 'Personal'. Spam should be deleted without opening or resending it, unauthorised software

should never be used and memory sticks or other portable media devices should only be used to remove non-confidential documents unless you have been given a BfN encrypted media device.

- Any equipment lost or stolen should be reported immediately.
- Any new equipment needs to meet these standards and comply with a formal privacy impact assessment where necessary.

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. Ideally, 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.

8.3 Mobile Phones

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.

8.4 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.

9. Records Management

BfN will continue to develop and improve good record systems based on the Nursing and Midwifery Council The Code: Professional standards and behaviour for nurses and midwives.as an example of best practise https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf We will also refer to the Records Management Code of Practice for Health and Social Care 2016 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. 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 (shredded).

Improving the quality of the information we hold is the key to improving the service we give to mothers and 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.

10. 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.

11. Information Governance– annual assessment of compliance

BfN is required to complete the Information Governance Statement of Compliance (IGSoC). The IGSoC process requires that organisations undertake an annual IG assessment using the IG toolkit. [Further details on the Connecting for Health website https://www.igt.hscic.gov.uk/]

IG assessments need to be submitted annually by 31st March 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 Statement of Compliance.

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

12. Training

All staff and volunteers are required to complete the relevant modules using the NHS Digital e-learning tool https://nhsdigital.e-lfh.org.uk/ and to undertake updates on an annual basis.

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

This is detailed in Appendix 6 and should be referred to in all cases where you suspect a breach may have occurred.

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/
    - 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
- BfN Records Guarantee http://www.breastfeedingnetwork.org.uk/wp-content/pdfs/governance/BfN_Records_Guarantee.pdf
- 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 https://www.igt.hscic.gov.uk/

Training slides https://www.igtt.hscic.gov.uk/igte/index.cfm

What you should know about

Information Governance

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance

The Care Record Guarantee https://digital.nhs.uk/services/registration-authorities-and-smartcards

Caldicott guidelines http://scot-ship-toolkit.org.uk/roles-and-responsibilities/caldicott-guardians

https://www.gov.uk/government/groups/uk-caldicott-guardian-council

Freedom of Information Act http://ico.org.uk/for-organisations/guide-to-freedom-of-information/

http://www.itspublicknowledge.info/home/ScottishInformationCommissioner.aspx

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

The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1]

It was adopted on 27 April 2016. It becomes enforceable on 25 May 2018, after a two-year transition period. The GDPR replaces the 1995 Data Protection Directive.[2]

Because GDPR is a regulation, not a directive, it does not require national governments to pass any enabling legislation and is directly binding and applicable

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;- be open, honest and clear

There should be no surprises, so inform data subjects why you are collecting their information, what you are going to do with it and who you may share it with eg when formulating a research project remember to be open and transparent about what you will be doing with the information. e.g. when working in a team, ensure that the mother is aware of who the members of the team are, and that all those involved with their care may need to see their notes.

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;- if in doubt, check first!

Only use personal information for the purpose(s) for which it was obtained. e.g. personal information on an Administration System must only be used for service use purposes - not for looking up friends' addresses or birthdays. Only share information outside your local team, committee, elist or service if you are certain it is appropriate and necessary to do so.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Only collect and keep the information you require. It is not acceptable to hold information unless you have a view as to how it will be used. Do not collect information "just in case it might be useful one day!" e.g. taking both daytime and evening telephone numbers if you know you will only call in the day.

- Explain all abbreviations
- Use clear legible writing
- Stick to the facts - avoid personal opinions and comments

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Take care inputting information to ensure accuracy

- How do you know the information is up-to-date?
- What mechanisms do you have for checking the information is accurate and up-to-date? E.g. each time you have contact with a Mother, they should be asked to confirm that their details are correct - address, telephone number etc. This can be simply done in a conversation with the Mother e.g. do you still live at [address], Have you changed your contact number since we last met?
- Check existing records thoroughly before creating new records
- Avoid creating duplicate records

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

- Follow retention guidelines. Check the relevant retention policy.
- Ensure regular housekeeping/spring cleaning of your information
- Do not keep "just in case it might be useful one day!"
- Check the relevant disposal policy
- Dispose of your information correctly

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

- Ensure security of confidential faxes by using Safe Haven/Secure faxes
- ALWAYS keep confidential papers locked away
- Do you have a clear desk policy?
- Ensure confidential conversations cannot be overheard
- Keep your password secret
- Ensure information is transported securely
- Good information management practices
- Guidelines on IT security
- Staff training
- Confidentiality clause in employment contracts
- Procedure for access to personal data

- A disposal policy/procedure for confidential information
- Confidentiality contracts with third parties e.g. archiving companies, cleaners, temporary staff, outside contractors e.g. Where BfN staff or volunteers are based in a children's centre

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

It is important that we are always able to:

demonstrate a good understanding of the personal information we hold,

show how our privacy information is communicated,

ensure that we have procedures in place covering all the rights of individuals, (see below)

demonstrate that we know our lawful basis for processing all personal information, (see below)

show that we have clear records of consent where this is our legal basis for processing,

be able to respond appropriately to a data breach (see Appendix 6)

The GDPR provides the following rights for individuals:

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

We must provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.

We must provide privacy information to individuals at the time we collect their personal data from them. We will do this by making people aware of our Privacy Policy and giving them access to this at the time we collect their information or by signposting them to our website.

The right of access - Subject Access Requests

Under the GDPR individuals have the right to access information which is held about them. Requests should be made in writing to the Paisley office or by email to admin@breastfeedingnetwork.org.uk Individuals who make a request are entitled to be:

told whether any personal data is being processed;

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;

given a copy of the information comprising the data; and given details of the source of the data (where available).

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 in any event within 30 days of receiving it. Information will be provided free of charge, except where a request is considered to be manifestly unfounded or excessive, particularly if it is repetitive, I which case a "reasonable fee" may be payable.

The right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

An individual can make a request for rectification verbally or in writing. Requests should be made in writing or by phone to the Paisley office or by email to admin@breastfeedingnetwork.org.uk

BfN will respond to rectification requests within one month of receipt

BfN will refuse to comply with any requests for rectification that are manifestly unfounded or excessive,

The right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'.

Individuals can make a request for erasure verbally or in writing. Requests should be made in writing or by phone to the Paisley office or by email to admin@breastfeedingnetwork.org.uk

BfN will respond to all requests within one month.

The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data.

This is not an absolute right and only applies in certain circumstances.

When processing is restricted, we are permitted to store the personal data, but not use it.

An individual can make a request for restriction verbally or in writing. Requests should be made in writing or by phone to the Paisley office or by email to admin@breastfeedingnetwork.org.uk BfN will respond to all requests within one month.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Requests should be made in writing or by phone to the Paisley office or by email to admin@breastfeedingnetwork.org.uk BfN will respond to all requests within one month. The personal data will be provided in a structured, commonly used and machine readable form.

The information will be provided free of charge.

The right to object

Individuals have the right to object to:

processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

direct marketing (including profiling); and

processing for purposes of scientific/historical research and statistics

Requests should be made in writing or by phone to the Paisley office or by email to admin@breastfeedingnetwork.org.uk BfN will respond to all requests within one month.

Rights in relation to automated decision making and profiling.

An individual can also request information about the reasoning behind any automated decisions, such as an assessment of performance at work. Requests should be made in writing or by phone to the Paisley office or by email to admin@breastfeedingnetwork.org.uk BfN will respond to all requests within one month.

Lawful Basis for Processing

The GDPR requires that we have a clear lawful basis for processing any personal information and that this is documented for all the personal information we collect and process. The following will normally apply to the information we collect:

Consent - We have the explicit consent of the data subject to process the information provided to us

Legitimate interests - Processing the data is necessary for the purposes of our "legitimate interests" as the data controller (except where such interests are overridden by the interests, rights or freedoms of the individual). This is likely to be most appropriate where we use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Contract - Processing the personal data is necessary for the purpose of carrying out a service level agreement/contract where we are commissioned to provide breastfeeding support services, or, Processing is necessary in order for us to fulfil a contract to deliver items or services ordered from our shop

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 Central Support Manager will decide whether any changes are necessary.

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
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

APPENDIX 5

PATIENT INFORMATION PROTOCOL OFFICE COPY

SEND THIS SIGNED AND DATED COPY TO: BfN, PO BOX 11126, Paisley, PA2 8YB

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)
5. Community coordinators will ring mums and get addresses again if they need to do home visits.
6. Peer Supporters 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 eg 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
- Research 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 20 MILLION EUROS OR 4% OF ANNUAL TURNOVER PER BREACH AND IMPOSE CUSTODIAL SENTENCES

PATIENT INFORMATION PROTOCOL

PROJECT COPY -KEEP THIS SIGNED AND DATED COPY WITH PROJECT RECORDS

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)
5. Community coordinators will ring mums and get addresses again if they need to do home visits.
6. Peer Supporters 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 eg 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
- Research 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 20 MILLION EUROS OR 4% OF ANNUAL TURNOVER PER BREACH AND IMPOSE CUSTODIAL SENTENCES

Peer Support Notification Form

Peer Support Programme Notification Form

** First Name:*	
** First part, plus the first number of Postcode e.g. PA2 1:*	
** Telephone number:*	

Number of weeks early, if baby born prematurely: _____

IMPORTANT

* indicates the **ONLY** details to be passed to the Project Lead/Coordinator by telephone.
Only the first half, plus the first number of the postcode is required.
All other details are to be communicated only in a private, face-to-face conversation.

Age Range: Under 20 ☐ ; 20 - 24 ☐ ; 25 - 29 ☐ ; 30 - 34 ☐ ; 35 - 39 ☐ ; 40 and over ☐

* Preferred Language: English ☐ ; Other ☐ (*please specify*)_____

Notifier (print name): _____

Designation: BfN volunteer/staff ☐ ; Midwife ☐ ; Health Visiting Team ☐

Children's Centre team ☐ ; Other (please specify)
_____

Date of Notification: _ _/_ _/_ _ _ _

APPENDIX 6

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

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 Central Support Manager. If it is not possible or appropriate to go via a Line Manager then the next point of contact is the Central Support Manager directly (contact details on our website). The Line Manager or the Central Support 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 Central Support 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 Central Support Manager of the steps you have taken to retrieve lost information or to minimise the risk of misuse such as:

a) Retracing your steps to see if you can find missing files or devices
b) If you have lost a mobile phone contact the provider and ask them to block access to the SIM
c) 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 Central Support 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. If BfN is considered to be the data controller this step should be handled by BfN with the support of the Central Support 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 Central Support Manager and Caldicott Guardian.