IT Policy and guidelines

Date of Issue:	March 2020	**Next Review Date:**	March 2022
Version:	1	**Last Review Date:**	March 2021
Author:		Central Support Manager	
Approval Route			
Approved By:		**Date Approved:**	
Shereen Fisher, CEO		March 2020	
Links or overlaps with other strategies/policies:			
Information Governance Policy			
Records Retention Policy (Annex 4)			
User Access Policy			
Staff Handbook			

Contents

1. Introduction 3
2. Scope of the Document 3
3. Aim of this Policy 3
4. Duties and Responsibilities 3
5. Acceptable Use 4
Authorised and Unauthorised Information Access 4
Misuse of Information Systems 4
Internet Acceptable Use 4
6. Guidelines for IT Equipment Use 5
Physical Protection 5
General Use 5
7. How to Get Help or Support 8

1. Introduction

This policy aims to:-

- Define processes to be employed in the protection, use and management of the BfN's Information Technology (IT) systems and resources.
- Ensure the application of best practice in line with Cyber Essentials accreditation and other guidelines

Information processing is fundamental to support the work of the BfN. As our use of IT systems continues to grow, the information we hold represents one of the BfN's most valuable and relied upon assets. It is essential that all computer systems and information are protected against the many and developing threats which may compromise them and so it is important for BfN to have clear and relevant policies and practices that enables it to comply with legislation, keep safe and confidential its sensitive information and minimise the impact of service interruptions.

2. Scope of the Document

This policy includes :

- Any device or equipment that connects to the BfN network which is capable of accessing, reproducing, storing, processing or transmitting information
- All information (digital, hard copy, photographic or audio) collected, processed, stored, produced and communicated through the use of IT resources by or on behalf of the BfN.
- IT information systems owned by or under the control of the BfN.
- The Breastfeeding Networks' systems, infrastructure and websites.
- All users (including employees, volunteers, agency & sub-contract staff, partner organisations, suppliers and customers) of the BfN's IT resources.

3. Aim of this Policy

The purpose of this policy is to establish an overarching framework, outlining the approach, methodology and responsibilities for IT security that provides assurance that:

- IT resources (including systems and the information contained within) are managed securely and consistently according to Cyber Essentials and other corporately specified standards and practices.
- Members of staff and volunteers are aware of their own responsibilities concerning security of the IT resources that they use
- Safe and secure IT environments are provided for storage and use of the BfN's information and that information is accessible only on a 'need to know' basis.
- Information security risks are identified and controlled.

4. Duties and Responsibilities

Staff and volunteers

Every member of staff and every volunteer is personally responsible for ensuring that no breaches of computer security result from their actions and shall:

- Comply with this policy, its related processes, guidelines and safe working practices.
- Ensure that they are fully aware of the unacceptable uses of IT resources as outlined in this policy.
- Understand their responsibilities to prevent theft, protect and maintain the confidentiality and integrity of the BfN's information assets and data and security of the BfN systems.
- Ensure operational security of the information and IT equipment and systems used.
- Receive adequate training or guidance in the use of any IT equipment or systems provided by the BfN in relation to their own duties and responsibilities.

- Comply with notifications that may be issued from time-to-time by Central Support concerning any collective or individual action that must be undertaken in response to potential or actual information security threats.
- Ensure that any incident that could potentially affect the security of information is reported in a timely manner.

5. Acceptable Use

5.1 Authorised and Unauthorised Information Access

- The BfN employees and volunteers **shall** only be authorised to access information relevant to their work as per the User Access policy.
- Accessing or attempting to gain access to unauthorised information **shall** be deemed a disciplinary offence.
- When access to information is authorised, the individual user **shall** ensure the confidentiality and integrity of the information is upheld, and observe adequate protection of the information according to BfN policies such as the IG policy, as well as legal and statutory requirements e.g. GDPR. This includes the protection of information against access by unauthorised persons.

5.2 Misuse of Information Systems

- Use of the BfN's information systems for malicious purposes **shall** be deemed a disciplinary offence. This includes but is not limited to:
  - Penetration attempts ("hacking" or "cracking") of external or internal systems.
  - Unauthorised electronic eavesdropping on or surveillance of internal or external network traffic.
  - Discriminatory (on the grounds of sex, political, religious or sexual preferences or orientation), or derogatory remarks or material on computer or communications media; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.
  - Acquisition or proliferation of pornographic or material identified as offensive or criminal.
  - Deliberate copyright or intellectual property rights violations, including use of obviously copyright-violated software.
  - Storage or transmission of large data volumes for personal use, e.g. personal digital images, music or video files or large bulk downloads or uploads.
  - Using the credentials of others for purposes, including, but not limited to, posing as another staff or volunteer member of BfN, accessing information or performing activities that are not otherwise possible.
- Users accessing or attempting to access confidential information concerning themselves, family, friends or any other person without a legitimate purpose and prior authorisation from senior management is strictly forbidden and **shall** be deemed a disciplinary offence.
- Use of BfN information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and **shall** be deemed a disciplinary offence.
- If identified misuse is considered a criminal offence, criminal charges **shall** be filed with local police and all information regarding the criminal actions handed over to the relevant authorities.

5.3 Internet Acceptable Use

- Whilst conditional personal use of some IT resources of the BfN is permitted (e.g. e-mail and internet), users should be aware that there must be no expectation of privacy when using devices owned by BfN, or when using BfN licenced software. If privacy is expected, BfN's IT resources must not be used for personal matters.
- Excessive personal use of the Internet during working hours **shall** not be tolerated and **may** lead to disciplinary action.
- Users **shall** not use Internet-based file sharing applications, unless explicitly approved and provided as a service.
- Users **shall** not upload and download private data (e.g. private pictures) to and from the Internet.
- Users **shall** not download copyrighted material such as software, text, images, music and video from the Internet.
- Users **shall** not use BfN systems or Internet access for personal advantages such as business financial transactions or private business activities.

- Users should take extra care when using public WiFi and when working in public places due to the risk of the theft of login credentials, or inadvertent sharing of sensitive information (for example, having confidential information clearly visible on a screen in a public place). Use of public WiFi is discouraged and should not be used when accessing personal, sensitive or confidential information.

6. Guidelines for IT Equipment Use

6.1 Physical Protection

- Users should take all reasonable precautions to ensure the physical security of all BfN devices and should be aware of the potential risk of spillages, magnetic fields, sudden impacts or excessive force.
- If left unattended in semi-controlled areas such as conference centres or customer offices, laptops **shall** be locked to a fixed point using a physical lock available from various sources, or kept with the BfN staff member at all times. If leaving the computer, it should be locked (using the Ctrl-Alt-Delete function) or switched off.
- Portable equipment **shall** never be left unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure.
- Portable equipment **shall** be physically locked down or locked away when left in the office overnight, and switched off.
- Portable equipment **shall** never be left in parked cars, unless completely invisible from outside the vehicle and protected from extreme temperatures.
- Portable equipment **shall** not be checked in as hold luggage when travelling, but treated as hand or cabin luggage at all times.

6.2 General Use

- Users **shall** lock their terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete function or other applicable method) when left unattended, even for a short period.
- Users **shall** not install unapproved or privately owned software on BfN IT equipment.
- Laptops and mobile devices **shall**:
  - Only be used by the BfN employee or volunteer that has signed and taken personal responsibility for the laptop.
  - Have a reputable and up to date anti-virus, anti-spyware and personal firewall software installed and activated.
  - Any device lost or stolen shall be reported immediately to Central Support
  - Personal data must not be held on portable media (including laptops, mobile phones or tablets), unless there is a definite need to do so and this has been approved by the Central Support Manager.
  - Users must ensure that valuable organisational data created or modified is backed up regularly, preferably onto OneDrive, but not only onto the hard drive of the device.
  - Any device used to access, store or process sensitive personal information must encrypt any data or store files on OneDrive. If it is absolutely necessary to store personal information on the hard drive this should be done within an encrypted section of the hard drive, using a system such as Veracrypt https://www.veracrypt.fr/en/Home.html .
  - The use of memory sticks/USB/external drives should be avoided as they are easy to lose and are not always adequately protected. Consider other ways, such as Office 365, to be able to access your files from different devices. Do not use USB sticks (or CDs, DVDs) provided by others or that you do not know the provenance of, as this is a common way of spreading malware.
  - All portable media used by BfN should be logged by Central Support to track its use and location.
  - 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.
  - In instances where IT (including removable media) equipment is to be allocated to a different user, or where it is to be repurposed, Central Support shall be consulted to advise upon and carry out necessary clearing and sanitisation prior to reassignment.

- At end of life, all IT equipment (including removable media) owned or controlled by the BfN shall be returned to the Paisley office for erasure of data and secure disposal in accordance with relevant standards and guidelines.

6.3 System specification, Operating System and System Updates

All operating systems should be up to date and all users should ensure that the operating system of any device connecting to BfN systems is still supported by the manufacturer. A list of current supported operating systems is provided in Annex 1.

If an operating system is supported, automatic system updates should be received and activated. It is very important that these are allowed to install as soon as possible, in all circumstances within 14 days, as they may contain protection against the latest threats.

6.4 Usernames, Passwords and PINs

All computers should be protected with a username and strong, unique password. Devices such as mobile phones should be protected with either a password or a secure PIN/fingerprint. User accounts that are no longer needed should be removed.

6.4.1 Setting passwords

- All passwords should be complex and difficult for unauthorised people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. Consider using three random words as a basis for your password. These requirements will be enforced with software when possible.
- In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective. “Breastfeeding” is also easy to guess given the context of our work.
- A password should be unique, with meaning only to the employee who chooses it. One method recommended by the National Cyber Security Centre is to use three random words, and change letters within those words to numbers or symbols.
- Employees must choose unique passwords for all of their work-related accounts, and may not use a password that they are already using for a personal account.
- All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question. Do not reuse or increment passwords when resetting (for instance, moving from “password1” to “password2” or from “BfNPasswordsummer2019” to “BfNPasswordwinter2020”): this practice is well recognised amongst malicious parties, meaning such passwords are easier to guess. This requirement will be enforced using software when possible.
- If the security of a password is in doubt – for example, if it appears that an unauthorised person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new employees when they start or those that protect new systems when they are initially set up — must be changed as quickly as possible.

6.4.2 Protecting passwords

- Staff may never share their passwords with anyone else within the organisation, including colleagues, managers, administrative assistants etc. Everyone who needs access to a system will be given their own unique password.
- Employees may never share their passwords with any outside parties, including partners or family members.
- Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. Try to avoid clicking on links and documents from

individuals and organisations that you are not expecting to receive such things from. If you are concerned, phone up the sender to verify prior to opening any links or attachments.

- Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.
- Employees may use password managers or other tools to help store and remember passwords.
- When configuring password "hints," do not hint at the format of your password (e.g. "postcode + middle name").
- User IDs and passwords must not be set to enable automatic login.
- "Remember Password" feature on websites and applications should not be used.
- All mobile devices that connect to the BfN systems such as email must be secured with a password or PIN and/or biometric authentication.

6.5 Firewalls

Most laptops come with a built-in firewall which provides basic protection from security threats and malware. For Windows, this should be switched on in Control Panel>Windows Defender Firewall. On a Mac, choose the Apple menu > System Preferences, click Security & Privacy, then click Firewall.

Some internet routers also come with Firewalls. Where available these should also be switched on; please refer back to your router's manual for further details on how to do this.

6.6 Antivirus

A reputable anti-virus software must be installed and active on any device used to access BfN systems or files. The software should be set to automatically update on a daily basis and these updates should be allowed to run in a timely manner in order to prevent risk from any new threats. The software should also be set to scan files automatically and to scan any websites for potential threats. Anti-virus is available centrally for those that need it. Please contact the Central Support Manager to arrange this.

6.7 Software

The more software installed on a device, the greater the risk of something becoming out of date and becoming vulnerable. It is advisable that only software and apps that are needed for your job are installed on any device used to access BfN files or systems. Any default programs that come with the device, such as games or apps for online shopping etc. should be disabled or removed. It is also recommended that for every software or system, users are given the lowest possible level of permissions necessary to do the job. For example, there is no need to have complete Admin rights if the job only involves data entry.

All software installed should be correctly licensed and supported by the supplier. Any software that is no longer licensed or supported should be removed. Discounted software can be purchased centrally, please contact Central Support for more information.

It is important that any automatic software updates are applied as soon as possible, in all circumstances within 14 days, as they may contain protection against the latest bugs and threats.

Only approved software/apps should be used to access BfN data such as files and emails. This list is included in Annex 1.

7 Bring Your Own Device (BYOD)

Ideally users requiring access to systems such as Office 365 or data records should be 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, with particular reference to the storage of personal data on OneDrive or on an encrypted section of the hard drive if agreed as being absolutely necessary
- Must not introduce unacceptable risks (such as malware) onto BfN networks (Office 365) 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
- Must notify BfN of any potential security issues which pose a risk to BfN systems or data, such as a virus attack, phishing attack or ransomware attack
- BfN has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete any organisational data held on the (encrypted) hard drive as required, as well as any data held in the cloud (Office 365).
- BfN reserves the right to access and examine any device believed to contain, or to have contained, confidential organisational data where necessary for investigatory or control purposes, for example where we believe confidentiality has been breached, there has been a serious data breach or where information has been used for malicious purposes.

While employees and volunteers 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, for example while providing IT support via remote access. 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 How to Get Help or Support

If you have any questions about this policy or other issue related to the use of IT systems and cyber security, these can be discussed with your Line Manager, Project Lead or Supervisor. Alternatively please contact the central team at the Paisley office or email cyber@breastfeedingnetwork.org.uk

Annex 1

Currently supported operating systems

Device name	Minimum operating system requirements
Laptop	Windows 10 Build number 1909 and above MAC OS 10.14 and above
Mobile phone/tablet	Android 9 and above iOS 9 and above

Approved apps/software that can be used by specified individuals (i.e. the person the file is shared with) to access BfN data

Microsoft Office including Outlook, Word, Excel
Google Drive including Sheets and Google Docs
Open Office
Libre Office