2017

Information Security Policy

MARCH 2017

DAVID HARRIS – DATA PROTECTION OFFICER

Contents

Introduction

As our work inevitably involves the use of both Personal Data (that of our users, volunteers and committee members), and Sensitive Data (background checks, plus medical/spiritual/financial data on our volunteers and end users) there are two significant threats we as an organisation face.

Firstly, damage or disruption to our activities. This is most likely to be in the form of non-targeted hacking of computer systems that we use, but may also be an attempt to steal financial or personal data that we hold.

Secondly, loss or theft of some of the personal data that we hold. As a result, we are subject to the Data Protection Act 1998, and even an accidental loss would still leave us liable (in November 2016, a historical society was fined after a member of staff had their laptop stolen).

This Policy is intended to address both concerns, and to render us compliant with Data Protection legislation.

What is the threat from hacking?

Every day there are attacks on small organisations; these are less likely to be targeted than those focussing on larger businesses, but are more likely to be effective. The government's Cyber Breaches Survey in 2016 revealed that 24% of all businesses had experienced one or more cyber breaches in the previous 12 months. Of these, 68% involved viruses, spyware or malware (e.g. "ransomware"); 15% involved denial of service (DDoS) attacks; 13% involved direct hacking of company computers, and 8% involved thefts of personal information. The mean number of breaches in the preceding 12 months for **all** small and micro-businesses was 15! The mean cost to small businesses was £3100.

For more information, see HM Government's "Cyber security: advice for small businesses" on:
https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know
and the Cyber Security Breaches Survey 2016:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

A successful theft of personal information could, if the Information Commissioner's Office deemed the company to be negligent in compliant with their legal obligations, result in a prosecution under the Data Protection Act. This could result in a fine of up to £500,000 and potentially personal prosecution of volunteers and committee members directly involved.

What is personal data?

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Typically, it might include a person's name, email address, or address.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data", and therefore controlled under the DPA.

What is Sensitive Data?

His category (also known as Sensitive Personal Data) comprises information as to -

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

(b) their political opinions,

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

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

(e) their physical or mental health or condition,

(f) their sexual life,

(g) the commission or alleged commission by them of any offence, or

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

Highlighted in **bold** are those definitions most likely to be of relevance to us. Because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

What are the main provisions of the Data Protection Act?

There are 8 Principles of Data Protection that all businesses holding such data must comply with:

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data Management and Security Responsibilities

All staff share responsibility for data security and data protection.

BMCN is a Registered Data Controller under ICO's jurisdiction.

Specific responsibilities are allocated as follows:

Data Protection Officer:

Responsible for data management policies, training and broad-brush compliance.

David Harris

IT Security Officer:

Responsible for IT security policies, training and compliance; and oversight of company IT systems.

David Harris

Records Management Officer:

Responsible for personal data queries and requests, and oversight of data management on a day-to-day basis.

Mark Alderson

Physical Security

Why is this important?

Sensitive Data:

All sensitive data is stored “offline” in secure locations. This data MUST be protected from unauthorised access.

Personal Data:

This data may be stored offline as above, or online.

No network or IT security system will protect data if an unauthorised person obtains access to the computers it is stored on (this is sometimes called the “Evil Maid” attack). As a result, it is vital that all computers containing BMCN data are secured appropriately. Note, this does **not** invalidate the requirements for data encryption etc. below, it is in addition to them.

Physical Security Protocol:

Sensitive and Offline Personal Data Records

This section applies to the main ("Primary") and backup copies ("Secondary") records maintained on each volunteer and end user.

All records will be stored at ALL TIMES when not actively being modified in a locked receptacle in a secure room within secured premises. Unauthorised persons will NEVER be permitted access to the receptacle, and only to the secured room under strict supervision.

Documents will NEVER be removed from the Primary store except for modifying or duplication, prior to transfer to the Secondary store; or for destruction (as obsolete and more than 7 years old). Documents will NEVER be removed from the Secondary store unless for destruction (as obsolete and more than 7 years old) or to restore the Primary database in the event of complete or partial data loss in the Primary store.

Personal Online Data Records

This section applies to any machine; any computer, tablet, phone or other mobile device that is used to access or store BMCN data.

1. When not in use, the machine must be stored securely:
    a. On your person (see also the Mobile Device Policy)
    b. In a locked room of a secure building
    c. In a permanently attended building where no person can obtain access to the room without attracting notice and being challenged.
    d. In a locker or other securely locked receptacle in a public place ONLY AS A LAST RESORT and if the site is under observation by a security guard or similar.
2. In any insecure place of use, portable machines (e.g. laptops) should be affixed to a secure object or structural member with a Kensington lock.
3. When being used in a public or semi-public place (e.g. an internet café) portable machines should NEVER be left unattended, secured or otherwise, unless in a locked room to which only BMCN and/or building security staff have a key.

Network and IT Security:

Why is this important?

Any networked computer is potentially vulnerable to attack by hackers. However, basic Network and IT security precautions can minimalize the risk. These include antivirus and antimalware software; strong software and hardware firewalls; maintaining up to date ("patched") software; regular cleaning or secure deletion of old files (especially .tmp files that may contain unencrypted data); secure access protocols (such as file encryption and regular password rotation); and network traffic monitoring (where appropriate).

When being used outside of a relatively secure environment (e.g. home or a secure office space), additional security is required. This may include specific protocols for users to follow, as well as a device record and the capacity to remotely wipe lost or stolen mobile devices.

There is also a Safe Working protocol for all users, intended to foster good IT security practice.

ICT Standard Protocols:

These protocols are intended to protect the **computers and other devices holding or having access to secure data**. All users MUST comply to these protocols.

BYOD machines ("bring your own device") – you agree to maintain these standard policies and systems on your own machines and networks, and to follow the standard protocols below.

Antivirus Protocols

All machines MUST run an appropriate and authorised antivirus and antimalware suite. This is to be fully installed and run constantly. Any abnormal behaviour of the software is to be reported immediately and if the problem is not resolved, the machine must NOT be used until the Breach Recognition Protocol has been followed.

BYOD machines – you agree only to use antivirus and antimalware software that exceeds 99% detection rates of both zero-day exploits and widespread malware, as defined by the most up-to-date AV-Test data.

As of 24/02/2017, suitable software includes:

AhnLab V3 Internet Security; Avast Antivirus (100/99.7); Avira Antivirus (100/99.6); Bitdefender Internet Security (99.3/99.9); ESET Internet Security (100/99.6); F Secure Safe (100/99.9); G Data Internet Security (99.3/100); Kaspersky Internet Security (100/99.9); McAfee Internet Security (99.0/99.8); Microworld eScan Internet Security (99.3/99.9); Norton Internet Security (100/100); Panda Security Protection (99.5/99.8); Trend Micro Internet Security (100/99.9).

Avira Free Security Suite is recommended free antimalware system.

Other software – provided it meets industry standards (98/99) may be acceptable in consultation with the IT Security Officer.

Software setup:

You will be responsible for ensuring that:

1. Software is set up so as to offer “Real Time Protection”
2. Regular automatic scans are performed
    a. If malware is found, instruct the software to remove the threat.
    b. If this is not possible, contact the IT Security Officer or the software manufacturer for advice.
    c. If there is a risk that data has been penetrated, follow the Breach Recognition Protocol.
3. If you have Microsoft Defender installed in addition to the above software (default on Windows 10), select the option in its setup menu to “allow periodic scanning”. This will result in a second scan of the computer, reducing the risk that malware will be able to become established by evading the primary software.

Firewall Protocols

All machines must run a suitable Software Firewall.

This is a programme that acts to prevent unauthorised access to the computer by external threats.

For most purposes, the Windows 8/Windows 10/OS X Firewall is adequate, running in default mode. It may, however, be necessary from time to time to modify the Firewall settings.

1. If you are ever asked whether to "allow or deny access" to a programme or file that you do not recognise, always instruct the Firewall to "Deny" access.
2. If there is any suspicion that your computer may have been compromised, follow the Breach Recognition Protocol.

If you are running another Firewall programme (e.g. one contained within an antivirus software package), you must follow the same protocols.

All connections must be through a Hardware Firewall

This is built into most home routers or hubs, and provides a second layer of defence.

1. Ensure that you have changed the default administrator password on your router
2. If there is any suspicion that your computer may have been compromised, follow the Breach Recognition Protocol.

If you are connecting to the internet through a router that you do not control or trust absolutely, you cannot assume that you are protected by a Hardware Firewall.

3. Follow the Protocol for Working on Unsecure Networks

Update and Patch Protocol

All software must be regularly updated to the latest and most secure version

This is known as “patching”, and is intended to ensure that any insecure code in the software is replaced as soon as it is discovered. This minimises the risk of hackers being able to access your computer by using a “zero-day exploit” – an unpatched defect in the code.

If you are running Windows 10, your computer will automatically receive updates and install them. Major updates usually come out on “Patch Tuesday”, the 2nd and sometimes 4th Tuesday of the month (US time, so it may be Wednesday in the UK).

1. Ensure that your computer is set to “install updates automatically”:
    a. Go to Windows/Settings/Update & Security/Windows Update.
    b. If there is no option to “delay” or “automatically install” updates, then they are turned on by default.
2. Update other software regularly
    a. You may be prompted to do so periodically by your internet security suite.
        i. If so, click “update” or “check for updates”
    b. If not, the software itself should automatically check for updates when starting
        i. Ensure you start each programme you regularly use from scratch at least once a week.
        ii. If it asks for permission to look for or install updates, give that permission.

System Cleaning Protocols

When files are deleted, they should be securely scrubbed, or purged, from the computer.

A simple file delete does not actually delete the file – instead, it tells the computer that it can overwrite that file with another one if and when it needs to. However, this means that the files are still recoverable from your computer. When deleting, it is therefore necessary to use a "secure file deletion" mode, which removes files and then replaces them with random data. This may be a single overwrite, 3, 5 or 7 or even more "passes". For most purposes, 3-pass deletion is sufficient to assume the file has been rendered irrecoverable.

1. When deleting a file, ensure it is securely deleted. There are two options:
    a. Right-click on it and select "shred", "scrub" or "securely delete" from the dropdown menu. This will work if your antivirus software has this function
    b. Use an alternative disc cleaning tool such as CCleaner to find and delete the files.
2. Periodically, securely delete your "Downloads" folder as above
3. Once a month (or more frequently if you are deleting large numbers of sensitive files) clean your hard drive of unwanted files, imperfectly deleted files, and .tmp files (this will also speed up your computer!).
    a. Open CCleaner
    b. In Options/Settings select "Secure File Deletion" and choose "Advanced Overwrite (3 passes".
    c. Go to the Cleaner broom icon
    d. Ensure the "Wipe Free Space" box is ticked and click "Analyse". When the analysis is complete (which may take some time) click "Clean" (which may take several hours, so do so overnight).

Secure Access Protocol

It is vital that only authorised persons have access to personal data or other secure files.

There are three components to this.

1. Computer login details
    a. The password for your computer should be suitably secure:
        i. A mixture of numbers, letters and if possible symbols
        ii. Not spelling out a dictionary word (even including letter substitutions)
        iii. A minimum of 8 characters long
    b. This password should be changed **at least** every 3 months.
2. File encryption
    a. Files containing Sensitive or Personal Data (e.g. files containing contact details, Safeguarding data, etc.) should be encrypted using Microsoft Password Protection
        i. File/Password Protection
        ii. Use an agreed password with other members of the team to ensure everyone has access to password protected documents
        iii. Remember to save the file after applying password protection
        iv. A password protected file CANNOT be accessed if the password is forgotten so make sure you enter it correctly!
    b. File passwords should be changed:
        i. At least every 6 months
        ii. If any member of the team reports a Data Breach
3. Disk encryption
    a. Computers containing Sensitive or large amounts of Personal Data may require disc encryption. This encrypts the entire hard drive with a password, making it very hard to access any data unless the user enters the correct password.
    b. This requires either Windows Professional (BitLocker) or third party software and is not currently considered routinely necessary for BMCN machines.

Network Traffic Protocol

It is possible to monitor network traffic to detect hacking attempts before they access any sensitive data.

This requires specialised “packet sniffing” software, and is currently not considered practical for BMCN, given our distributed working practices.

Mobile Working Policy:

It may periodically be necessary to access Personal or even Sensitive Data away from a secure environment (defined as a secure room, not overlooked for physical documents; and an environment behind a secured access point with a controlled hardware firewall for digital data).

In these situations, you must follow this protocol:

Offline Data:

1. Avoid if at all possible
2. Ensure that the data is secured within a lockable carry case or similar – a 6 digit combination code is acceptable.
3. Ensure it is not possible that you will be overlooked - make sure that no-one can observe over your shoulder
4. Count documents out of the locked case and count them back in to ensure none have been left behind
5. NEVER leave the locked case unattended, keep it on your person at all times
6. Return data to the Primary or Secondary store as soon as possible
7. Record the fact that data has been removed to an unsecure environment on the Data Log

Online Data:

See below for the Protocol for Working on Unsecure Networks

Risk Analysis

Type of Data	Probability of Loss	Severity of Loss	Overall Risk
Offline Sensitive	Low	High	High
Online Sensitive	Medium	High	HIgh
Offline Personal	Low	Low	Low
Online Personal	Medium	Low	Medium

The highest protection must therefore be accorded to Sensitive Data.

Protocol for Working on Unsecure Networks

When working on an unsecure network (e.g. 2G, free wifi, etc), there is a significant risk that data transmitted (e.g. as an email, or logins for a website) will be intercepted by "packet sniffers". When working on these networks, follow the following protocol:

1. Avoid if at all possible
2. If not, use a VPN (Virtual Private Network).
    a. There is a free system bundled with Avira
    b. The other recommended free programme is Hotspot Shield Free
    c. This will encrypt your connection, keeping the data safe.

Device Register

The following devices have access to BMCN Online Personal Data:

Device	Data held/accessed	Notes
Mark's Desktop	Personal Data Referrals	
Emma's Mac	Personal Data	
Mary's PC	Safeguarding Data	
Rob's PC	Personal Data	
David's Laptop	Privacy Requests	

Device Control

Any portable devices (e.g. tablets, phones, laptops) carrying Online Sensitive Data must be capable of being remotely wiped in case of theft or loss.

This is highly recommended for devices holding Personal Data as well.

Code of Conduct:

All users agree to abide by the Code of Conduct when using machines that hold or are used to access BMCN data.

This is essential to maintaining data security. If you make a mistake, don't worry – we're all human! – but please report it AS SOON AS POSSIBLE so the Breach Risk can be assessed.

Safe Working Protocols

1. Run up-to-date and effective security software.
2. Patch their system regularly.
3. Use industry-standard file deletion utilities (e.g. CCleaner) to remove old and unwanted files.
4. Avoid the use of suspicious or dubious websites (to minimise the risk of “drive-by” downloads). Such sites may include freeware, click-bait or pornographic sites, among others.
5. Report any possible breaches to the Data Protection Officer IMMEDIATELY.
6. NEVER click a link in an email or other electronic message unless you are CERTAIN you know the sender.
7. NEVER enter passwords into a form or website accessed by clicking a link on an email – instead, load up the website directly on your browser and log in through that.

Password Policy

1. The password for your computer and for any Personal Information files should be suitably secure:
    i. A mixture of numbers, letters and if possible symbols
    ii. Not spelling out a dictionary word (even including letter substitutions)
    iii. A minimum of 8 characters long
2. Computer passwords should be changed **at least** every 3 months.
3. File passwords should be changed **at least** every 6 months.
4. If a breach is reported, passwords should be changed IMMEDIATELY.

Breach Recognition and Management:

If a Data Breach occurs, or is even suspected, it must be reported to the Co-ordinator (Mark Alderson) and Data Protection Officer (David Harris) IMMEDIATELY.

The Breach Management Protocol must then be followed.

A Data Working Group will be convened to assess:

1. The probability that a data loss has indeed occurred
2. The severity of such loss
3. Suitable actions

Information Security Risk Analysis

This matrix may be used to assess the severity of a suspected data breach.

1. Does the lost data include information on the subject's:
    a. Mental or physical health?
    b. Religious or personal beliefs?
    c. Finances?
    d. Criminal Record (or allegations of same)?

    If yes, this is a **Breach of Sensitive Data**.
2. Does the lost data include information on the subject's:
    a. Name?
    b. Email address?
    c. Physical address?
    d. Phone number?
    e. Any other information that could identify them?

    If yes, this is a **Breach of Personal Data.**

Protocol for Data Breaches

If a data breach is suspected, reported or proven:

1. Establish a Data Working Group
    a. This will comprise:
        i. The Coordinator (Mark Alderson)
        ii. The Data Protection Officer (David Harris)
        iii. The Safeguarding Officer (Mary Lovell)
        iv. The Volunteer (if relevant)
        v. The person who detected the suspected breach
        vi. Any other relevant person.
    b. It must meet – physically or virtually – within 24 hours of a suspected breach being reported.
    c. They will decide if it is **probable** (not certain) that Personal or Sensitive Data has been stolen or lost.
    d. If so, they must attempt to ascertain the proximate and ultimate causes.
2. **Breaches of Sensitive Data:**
    a. The Police must be contacted to report the loss.
    b. The data subject (or, where appropriate, their next of kin or primary carer) must be informed of the suspected loss.
    c. The PCC must be informed, as should the Insurers (Ecclesiastical).
    d. It may be appropriate to contact the Information Commissioner's Office.
    e. If a weakness in systems, protocols or any other security measure is deemed to be at fault, this must be rectified IMMEDIATELY
    f. In the event of a physical breach, all keys should be changed; in the interim, it may be necessary to move the breached store to a new location for safe-keeping.
    g. In the event of a digital breach, all computer and file passwords must be changed.
3. **Breaches of Personal Data:**
    a. The data subject (or, where appropriate, their next of kin or primary carer) must be informed of the suspected loss.
    b. The PCC must be informed, as should the Insurers (Ecclesiastical).
    c. If a weakness in systems, protocols or any other security measure is deemed to be at fault, this must be rectified IMMEDIATELY
    d. In the event of a physical breach, all keys should be changed; in the interim, it may be necessary to move the breached store to a new location for safe-keeping.
    e. In the event of a digital breach, all computer and file passwords must be changed.

Records of Data Breaches

Date of Breach	Data Lost	Suspected Cause	Actions Taken

Data Storage and Record Management Policy:

It is essential that all data stored is recorded below, and filed appropriately to ensure it is:

1. Trackable
2. Findable
3. Updatable

Privacy Policies:

For End-Users (“clients” or “carees”)

This information must be made available when they have their home assessment.

For Volunteers

This information will be available on the Website and in the Information Pack

End User Privacy Policy

To provide you with the pastoral care you need, BMCN has to collect certain data about you. This notice informs you of what information we keep, how and why we use it, and who to contact if you have any questions.

What information is being collected?

We store your contact details, how to find you, and information about your healthcare needs. We may also keep information about your personal religious or spiritual beliefs (if you choose to share these with us), your next of kin or carer(s), and anything you choose, in confidence, to share with us to allow us to help care for and support you.

Who is collecting it?

The volunteers and Coordinator of Brentor & Moor Compassionate Neighbours, an autonomous subcommittee of the Brentor Parochial Church Council.

How is it collected?

Our Coordinator and Volunteers will fill out a questionnaire when they first visit; any other information you choose to share will be added to this as appropriate.

Why is it being collected?

To allow our volunteers to help and support you with your chronic health needs, and as you approach the end of life.

Who will it be shared with?

We do not share this information with any other party, including the Brentor PCC, unless you ask us to. We do not sell or trade your information.

We may share it with the local medical services if this should be necessary (for instance, should you become suddenly ill), or with the police or fire brigade in an emergency or if required by law to do so.

What will be the effect of this on the individuals concerned?

There should be no impact on you except that we are able to help support you effectively.

How can I find out what information you keep?

Contact the Data Protection Officer (David Harris, email bmcneighbours@gmail.com, or telephone 01822 810845).

Can I object to any information you keep on me?

Yes – contact the Data Protection Officer and let them know what information you object to. They will respond with a formal response within 14 days (any usually much sooner).

Staff and Volunteer Privacy Policy

To support you, protect you, and protect our end-users, BMCN has to collect certain data about you. This notice informs you of what information we keep, how and why we use it, and who to contact if you have any questions.

What information is being collected?

We store your contact details, your relevant qualifications, experience, training needs, date of birth, safeguarding information and other information from your Application Form. In addition, any other information you choose to share with us.

Who is collecting it?

The Coordinator and Recruitment Team of Brentor & Moor Compassionate Neighbours, an autonomous subcommittee of the Brentor Parochial Church Council.

How is it collected?

On your Application Form and in your interview, in addition to any other information you may choose to share with us.

Why is it being collected?

So that we can contact you, and to protect our end-users.

Who will it be shared with?

We do not share this information with any other party, including the Brentor PCC, unless you ask us to. We do not sell or trade your information.

We may share it with the local medical services if this should be necessary (for instance, should you become suddenly ill), or with the police or fire brigade in an emergency or if required by law to do so.

What will be the effect of this on the individuals concerned?

There should be no impact on you except as pertains to your duties as a BMCN volunteer.

How can I find out what information you keep?

Contact the Data Protection Officer (David Harris, email bmcneighbours@gmail.com, or telephone 01822 810845).

Can I object to any information you keep on me?

Yes – contact the Data Protection Officer and let them know what information you object to. They will respond with a formal response within 14 days (any usually much sooner).

Data Collection Policy

Data Collected will include:

End Users:

- Name
- Address
- Contact Number
- Next of Kin and/or Primary Carer (if appropriate)
- Referring Organisation (if appropriate)
- Outline Medical Needs
- End User Assessment
- GP's details
- Any specific requirements
- Any religious or spiritual requirements (if appropriate)
- Any other information they choose to share with us

End User Data is NOT to be filed by their name or address. Instead, a Unique Reference Number in the following format is to be used:

BMCN – [Year] – [User Number]

So, for the first User in 2017, the Unique Reference will be BMCN-2017-01, and so on.

Volunteers:

- Name
- Address
- Contact details
- Relevant Qualifications
- Relevant Experience and Employment
- Training Logs
- End User lists and rotas
- DBS and Safeguarding Information

Physical files to be referenced in the same way, in the format:

BMCN-V-[Volunteer Number]

Data Retention Plan:

- **Personal Information – Volunteers**
  - To be kept on file until 7 years after the volunteer made their last visit.
- **Sensitive Information – Volunteers**
  - To be kept on file until 7 years after the volunteer made their last visit.
- **Personal Information – End Users**
  - To be kept on file until 7 years after their last visit.
- **Sensitive Information – Volunteers**
  - To be kept on file until 7 years after their last visit.

Data Record

Name	Data Kept	Location
Volunteers		
End Users		

Data Disposal Protocol

Physical Files

Cross Shred and Burn

Electronic Files

Scrub / Securely Delete data with a minimum 3x Overwrite Protocol

Data Destruction Schedule and Log

Dataset	Location	Date for Destruction	Destroyed On

Data Access Controls:

It is important that ALL access to Sensitive and Personal Data is recorded and logged.

Access Privileges

Only “Need to Know” personnel have access the data.

For Volunteer Personal Data, this comprises:

- The Coordinator
- The Secretary
- The Recruitment Committee
- The Safeguarding Officer

For End User Sensitive and Personal Data, this comprises:

- The Coordinator
- The Volunteer
- The Secretary (if needed)
- The Safeguarding Officer (if needed)

Data Logging Protocol

Electronic Data:

All logins to the Google Drive or Email Account should be logged by the Administrator

Physical Data:

A sign-in/sign-out sheet must be provided, requiring persons accessing the data to supply the following information:

1. Date of access
2. Person accessing (including printed name and signature)
3. Reason for access
4. Data accessed

Superencryption Policy

If Personal or Sensitive Data must be stored in an electronic format, it MUST be encrypted with a suitable password (see Password Policy). Microsoft Office applications (2007 onwards) have this capacity as default and it is highly secure.

Personal Data Request Protocol:

If a person wishes to enquire as to the data held on them, they should, in the first instance, contact the Data Protection Officer.

End Users

1. End-user or their carer contacts the Data Protection Officer
2. Data Protection Officer convenes a Data Working Group for specific advice
3. Within 14 days, the Data Protection Officer must respond to the enquiry:
    a. Providing the information
    b. Refusing the information ONLY IF there is sufficient ethical and legal justification to do so
4. If the End User or their carer wishes to challenge the information, the Data Working Group will reconvene and will respond corporately after, if necessary, taking relevant legal advice.

Staff and Volunteers

1. Staff member or volunteer contacts the Data Protection Officer
2. Data Protection Officer convenes a Data Working Group for specific advice
3. Within 14 days, the Data Protection Officer must respond to the enquiry:
    a. Providing the information
    b. Refusing the information ONLY IF there is sufficient ethical and legal justification to do so
4. If the staff member or volunteer wishes to challenge the information, the Data Working Group will reconvene and will respond corporately after, if necessary, taking relevant legal advice.

Data Transmission and Transferral Protocols:

Data must ONLY be transferred in a secure and safe format. It is not anticipated that data transfers will be routine except for:

1. Applications as volunteers
2. End-User referrals
3. Medical referrals
4. Backups from Primary to Secondary store

Data Transfer Protocol

Electronic Data:

- Must be transmitted in an encrypted format
- Password must be transmitted by a different route, e.g. telephone or in person
- NEVER store unencrypted data on a datastick or removable storage device

Physical Data:

- Transferred only in a lockable case or similar receptacle
- NEVER left unattended – it must remain on the person of the transferring official
- Moved directly from secure store to secure store
- If copying is required, this must only be done by a private or secure, if possible non-networked, photocopier.

End User Status Updates:

This information will need to be transferred to the Coordinator and the Primary secure store by the Volunteer. The protocol is as follows:

1. Volunteer visits End-User
2. Volunteer telephones the Coordinator's BMCN line
3. Volunteer leaves message asking Coordinator to phone them back
4. Coordinator replies; Volunteer gives any updates verbally
5. Coordinator updates files

Data Protection Analysis

If all policies are followed, the risk of a breach is estimated as very low. The highest risk is considered to be inadvertent loss of electronic data in transit (e.g. by email) due to staff carelessness in handling data. As we do not intend to store Sensitive Data in this manner, the severity of such a breach is considered to be low; however, training of all Volunteers and Committee Members will be instituted.

Privacy Proof Protocol:

Before any change to the operations or protocols of BMCN is implemented, a Privacy Impact Assessment will be carried out, using the below template.

Privacy Impact Assessment Protocol

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

For further information, see https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Operational Continuity:

All electronic records are stored on Google Drive or in gmail. This is an IMAP account with a remote server; the information is protected by the EU-US Privacy Shield.

Certificate: https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI

Thus, loss of any one machine will NOT impair operations.

Physical files will be backed up AT LEAST EVERY 2 WEEKS from the Primary to the Secondary Store. The Secondary Store to be held in a secure location physically separate from the Primary Store. Keys to be held by the Coordinator and the designated Data Backup Holder.

Backup Log

Dataset	Date Updated	Date Transferred to Secondary Store

Staff Education Policy:

To protect your data, that of your colleagues and our End-Users, it is vital that all staff are up-to-date with Data Protection legislation and policies.

Education Resources

1. All staff and volunteers must read and sign consent to this Information Security Policy
2. All staff and volunteers must watch and certify that they have watched the ICO training videos "Data Day Hygiene" and "Lights are On" here: https://ico.org.uk/for-organisations/improve-your-practices/training-videos/ NB – it is not necessary to watch the others unless you really want to!
3. Any staff with further training requirements or concerns should contact the Data Protection Officer (David Harris)

Training Log

Staff Member/Volunteer	Training	Signed/Date

Compliance Log

Date	Event	Certified
14/4/17	Launch – Data Protection Policy Launched	
1/7/17	Data Protection Policy Initial Review	
1/7/18	Data Protection Policy Annual Review	