



Data Protection Compliance Policy

National Back Exchange

Responsible Person

Sarah Thornton, Chair

Authors

Kerry Kemp, Vice Chair

Mary Muir, Publications Director

Contents

1. Version Control Summary	3
2. Introduction	4
3. Context and Scope	4
4. Data Protection Principles	5
5. General Provision	5
6. Lawful, Fair and Transparent Processing	5
7. Lawful Purpose	6
8. Data Minimisation	6
9. Accuracy	6
10. Archiving and Removal of Personal Data	6
11. Security	6
12. Breach	6
13. Roles and Responsibilities	7
14. Related Policies, Procedures and Guidance Documents	7
15. Policy Review	8
16. Audit – Monitoring Process	8

1. Version Control Summary

Date	Version no.	Summary of changes	Consulting group/person
July 2018	1.0	Privacy and Information Policy – new policy	S Love Chair N Sharpe, Vice Chair Professional Affairs Committee Members
March 2019	1.1 (1.a)	Additional comment to section 9 of the policy regarding NBE members not sharing website login details	N Sharpe, Vice Chair of National Back Exchange Board
July 2019	1.2 (1.b)	Minor changes to section 9 of the policy	N Sharpe, Vice Chair
May 2020	1.3 (1.c)	Reviewed no changes made to policy	N Sharpe, Vice Chair
October 2020	1.4 (1.d)	Removal of National Back Exchange Towcester office address	S Thornton, Vice Chair
November 2021	1.5	Reference to NBE Executive change to Board of Trustees	S Thornton, Vice Chair
November 2024	2.0	Major change – reviewed, redrafted, and renamed in line with NBE becoming a Charitable Incorporated Organisation (CIO) charity number 120 2540 - 29 th of March 2023. National Back Exchange Data Protection Compliance Policy	S Thornton, Chair K Kemp, Vice Chair M Muir, Publication Director

2. Introduction

This Data Protection Compliance Policy establishes a platform for how National Back Exchange (NBE) processes and protects personal data and other sensitive information.

This policy will operate as a framework for data protection, describe the basic principles of handling personal data, and instruct on how to use hereto connected guidelines and documents.

It is important that information is efficiently managed, and that appropriate accountability and supporting documentation provide a robust governance framework.

This policy is intended to safeguard NBE as an organisation, the Board of Trustees, members, partners, contractors, suppliers, and owners of intellectual property rights from information security-related incidents and any consequential action, loss of income, or damage.

The policy also aims to establish control measures informed by the [Information Commissioner's Officers guidance](#) and [The Data Protection Act 2018](#).

3. Context and Scope

This policy applies to all NBE Board of Trustees, members, partners, contractors, and suppliers who undertake any activity for NBE. It covers all aspects of information use within NBE including:

- Trustee, member, partners, contractors, and suppliers' information.
- Charitable Incorporated Organisation (CIO) information.
- Delegate information for events.
- Information required to deliver a service i.e. process and fulfil a publication order.
- Research and development information.

This policy covers all aspects of handling information including, but not limited to:

- Structured record systems - both paper and electronic.
- Transmission of information: including by email, digital (advertisements, blogs, Column, newsletter, sponsorship), verbal (meetings, webinars, events, which may be recorded for future viewing/reference, etc.), website, website community forum, social media platforms, telephone, text message, instant messaging platforms, post, fax, or other electronic methods.

This policy covers all information systems purchased, designed, developed, and managed by or on behalf of NBE and any individual acting as a Trustee or otherwise contracted or engaged as a volunteer by NBE.

4. Data Protection Principles

National Back Exchange is committed to managing and processing data in accordance with its responsibilities under the General Data Protection Regulations (GDPR).

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

- Processed lawfully, fairly, and in a transparent manner in relation to individuals.
- 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.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased, or rectified without delay.
- Kept in a form that 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 the implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.”

5. General Provision

- This policy applies to all personal data processed by National Back Exchange.
- The National Back Exchange’s Board of Trustees Chair and designate will be responsible for the ongoing compliance with this policy.
- This policy shall be reviewed annually.
- National Back Exchange shall register with the Information Commissioner’s Office as an organisation that processes personal data.

6. Lawful, Fair and Transparent Processing

- To ensure its processing of data is lawful, fair, and transparent, National Back Exchange shall maintain a Data Systems Register.
- The Data Systems Register will be accessible on National Back Exchange Google Drive and managed by the Associations Administration team which provides reports to the Board of Trustees Chair as required.
- Individuals have the right to access their personal data, and any such requests made in writing to National Back Exchange shall be dealt with promptly. This

information request may be a chargeable service depending on the length of time the request takes to secure the required information.

7. Lawful Purpose

- All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests ([see ICO guidance for more information](#)).
- National Back Exchange shall note the appropriate lawful basis in the Data Systems Register.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be available, with systems in place to ensure such revocation is reflected accurately in the National Back Exchange's systems.

8. Data Minimisation

- National Back Exchange shall ensure that personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

9. Accuracy

- National Back Exchange shall take steps as far as is reasonably practical to ensure personal data collected, transmitted, processed, and stored is accurate and kept up to date.

10. Archiving and Removal of Personal Data

- National Back Exchange will refer to the Data Retention and Deletion procedure in Appendix 1 and associated policies.

11. Security

- National Back Exchange shall ensure that personal data is stored on secure servers that are regularly maintained.
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted, this should be done safely such that the data is irrecoverable.
- Appropriate backup and disaster recovery solutions shall be in place.

12. Breach

- In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data, National Back Exchange shall promptly assess the risk to people's rights

and freedoms and if appropriate report this breach to the ICO ([more information on the ICO website](#)).

13. Roles and Responsibilities

It is the responsibility of all users of NBE information sources and systems to comply with statutory instructions regarding the safeguarding of information.

All relevant policies and procedures will be available to the members via the NBE website.

NBE understands its roles and responsibility for keeping up to date with current data protection requirements, and managing information correctly:

Data Protection Officer.

- The DPO (*NBE Board of Trustees Chair*) is responsible for data protection assurance and compliance within the National Back Exchange.

Information Asset Owner (IAO)

- The Information Asset Owner (IAO), (Associations Administration team acting on behalf of the National Back Exchange), are designated with the responsibility of maintaining, registering, and safeguarding NBE's information assets. This includes ensuring the integrity, confidentiality, and availability of the data. However, the overarching accountability for these information assets remains with the National Back Exchange Board of Trustees. This ensures that strategic and operational risks are managed effectively and that NBE's interests are always prioritised

Information Asset Administrators (IAA's)

- The IAA (*Associations Administration team*) is responsible for the day-to-day management of data, databases, or systems.

All members, partners, contractors, and suppliers

- All members, corporate partners, contractors, and suppliers are responsible for ensuring that they are aware of the data protection compliance requirements incumbent upon them and for ensuring that they comply with these on a day-to-day basis.

14. Related Policies, Procedures and Guidance Documents

Policies

- Privacy Notice
- Social Media Policy

Procedure

- Data Retention and Deletion Procedure

Internal NBE information

- Data Systems Register
- Google Drive Folder Register
- Data Review Log

Guidance

- Board of Trustees Handbook

15. Policy Review

This policy will be reviewed by the Chair, Vice Chair, or designates of the National Board of Trustees every 2 years from the date of publication or earlier depending on legal requirements, best practices, national guidelines, or organisational changes.

16. Audit – Monitoring Process

Monitoring process	Requirements
Who	<ul style="list-style-type: none">• National Back Exchange Chair• Association's Administration Team
How	<ul style="list-style-type: none">• Annual review of NBE data protection compliance policy, ensuring that NBE remains compliant with data protection laws and mitigates risks associated with data breaches.
Presented to	<ul style="list-style-type: none">• Board of Trustees
Monitored by	<ul style="list-style-type: none">• Sarah Thornton, Chair• Kerry Kemp, Vice Chair• Mary Muir, Publications Director• Association's Administration Team
Completion / Exception report to	<ul style="list-style-type: none">• Extraordinary circumstances beyond the control of National Back Exchange and/or Association's Administration Team