# National Back Exchange

# Privacy and Information Governance Policy


Contact: Administration Office
National Back Exchange
Linden Barns
Greens Norton Road
Towcester
NN12 8AW

Tel: 01327 358855
Email: admin@nationalbackexchange.org
Website: www.nationalbackexchange.org



Version: 1
Adopted: July 2018

**Contents** **Page**



© National Back Exchange 2018

## 1. Introduction

This document sets out the policy for National Back Exchange (NBE) to handle information, and provide guidance and tools associated with the use of confidential and person identifiable information.

It is important that information is efficiently managed and that appropriate accountability, standards, policies and procedures provide a robust governance framework for information management. Information Governance includes the requirement to measure compliance and produce year on year improvement plans.

This policy is intended to safeguard NBE as an organisation, staff, volunteers, members, Honorary officers and Executive committee members 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 requirements on network systems, based on the International Standards ISO/IEC 27001 and ISO/IEC 27002.

## 2. Scope

This policy applies to all NBE staff, members, volunteers and contractors who undertake any activity for NBE. It covers all aspects of information use within NBE including but not limited to:

- Member information
- Employee information
- Research and development information
- Corporate Information

The Policy covers all aspects of handling information including, but not limited to:

- Structured record systems -both paper and electronic
- Transmission of information: including by fax, email, post, telephone or other electronic methods

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

This policy also applies to anyone utilising the NBE social media pages, electronic platforms as well as present and future internet presences associated with NBE

## 3. Objectives

This Policy aims to provide:

- NBE employees, volunteers and members with a framework for the management of NBE information assets

© National Back Exchange 2018

- Assurance that relevant legal requirements are met with support for the provision of high quality member experience by promoting effective and appropriate use of information,
- Guidance and tools for employees processing confidential and person identifiable information
- Volunteers and employees with the tools to work closely together, preventing duplication of effort and enabling more efficient use of resources across NBE
- Procedures for the proper storage, protection and security of information and compliance with any third party partners requirements

## 4. Responsibilities

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

It is the responsibility of all users of NBE IT equipment, sources, systems and platforms to comply with the Prevent Duty and the related guidance.

NBE routinely uses Social Media and email to make members aware of the Policy and to inform them of any significant revisions to the Policy.

NBE understands its responsibility for managing information correctly. Such information management promotes business efficiency (recognising information as a primary asset, worthy of protection), effective risk management, legal compliance (especially in relation to the Data Protection Act) and sound corporate governance.

## 5. Roles

**IT Security Manager (Research, Information & Website Officer)**

The IT Security Manager is responsible for the management of information security in NBE and the strategy for Information Security requirements.

**The Data Protection Officer (Executive Chair)**

The Data Protection Officer takes the lead on Data Protection and advice on access to members Records and policy development and compliance.

**Information Asset Owners (IAO) (Local Group Affiliated Chairs)**

Chairs of NBE Local groups will oversee the issues of compliance with Information Governance requirements in their local group. They will ensure an Information Asset Owner with responsibility for particular Information assets is identified in the local committee structure. If no-one is allocated to this role, then it remains the responsibility of the local group Chair. IAOs are responsible for implementing procedures to minimise risk e.g. risk of fraud / theft / disruption of critical systems and provide assurance that information is being correctly managed

**Data Stewards (Social Media Volunteers)**

The Information Asset Owner can delegate to the data steward the responsibility for

© National Back Exchange 2018

overseeing the information asset life cycle. They are typically the process experts within their areas.

**Information Asset Administrators (IAA's)**

IAAs are appointed by NBE with day to day responsibility for managing risks to information assets and can be responsible for one or more individual databases or systems.

**Executive Committee Members**

All Executive Committee Members within NBE are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. It is their responsibility to ensure that individuals are made aware of their responsibilities through documentation.

**All Staff, Volunteers and Members**

All employees, volunteers and members whether permanent, temporary or contracted, are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Any individual, carrying out work on behalf of NBE, has a personal responsibility to comply with the law and with provisions laid down in their contracts of employment as well as NBE policies and procedures and documented best practice.

## 6. Key Governance and Security Elements

There will be proactive management of information within NBE and with other partner organisations, for member experience, service management and research as determined by law, statute and best practice.

Information security management has three basic components:

- Confidentiality: Protecting sensitive information from unauthorised disclosure
- Integrity: Safeguarding the accuracy and completeness of information and information processes. This involves identifying key data and rigorously maintaining version control
- Availability: Ensuring that information key to the business of NBE is accessible in a timely fashion

There will be a commitment to openness, through a Freedom of Information Publication Scheme, which involves making non-sensitive information publically available in line with responsibilities under the Freedom of Information Act 2000.

Effective arrangements are in place to ensure the confidentiality, security and quality of personal and other sensitive information and to ensure information within NBE is of the highest quality in terms of accuracy, timeliness and relevance.

NBE will ensure it;

- Holds information securely and confidentially
- Obtains information fairly and efficiently
- Records information accurately and reliably

© National Back Exchange 2018

- Uses information effectively and ethically
- Shares information appropriately and lawfully

## 7. Information Governance Framework

NBE Information Governance framework provides a consistent way for employees and members to deal with the many different information handling requirements, which include;

- Information Governance Management
- Confidentiality and Data Protection (including the Data Protection Act 2018)
- Information Security
- Member Records Management
- Research and development requirements
- Corporate Records Management (including the Freedom of Information Act 2000)

The framework allows NBE to ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible member experience and outcomes.

## 8. Records Management

NBE will ensure that all employees and volunteers are aware of their individual responsibility regarding member and corporate record issues. The Information Asset Owners and Administrators play a key role in ensuring that all creation, filing, indexing, storage, disposal and archiving of member and corporate records satisfy the highest practical standards for records management.

## 9. Confidentiality and Data Protection

NBE will ensure that all employees and volunteer members are aware of their individual responsibilities regarding data protection and confidentiality issues and also aware of how the area links with the broader Information Governance agenda.

NBE is responsible for security and confidentiality of personal information it processes. NBE will ensure that all relevant employees and volunteers are aware of their individual responsibility regarding processing of information and registration requirements.

Processing may include the transfer of information to countries outside the European Economic Area (EEA). In this case a transfer will not be made unless that country has an adequate level of protection for the information and or the rights of individuals. NBE will review the flow of member and personal information from NBE to ascertain if any such information flows outside the EEA.

## 10. Notification of Breach

Executive Committee members are responsible for recording actual or near miss incidents

© National Back Exchange 2018

involving any aspect of Information Governance. They will report Information incidents by sending details to the Executive Chairman or another member of the Executive committee who will categorise the severity of the breach and record the action taken.

Third party contractors, partners or provider organisations are required to notify NBE immediately if a breach, or suspected breach, occurs that may involve NBE information. All contracts with third parties and suppliers are required to have appropriate reporting clauses in their organisational policies and procedures.

With regard to personal data (i.e. data relating to an identifiable living individual) any suspected unauthorised disclosure should be reported to the Executive Chair, who is responsible for NBE's compliance with the Data Protection Ac

## 11. Business Continuity

Information security forms part of a wider business continuity context within the NBE.

The Executive Committee will ensure all information systems are documented so that should they fail, or if there is a breach from external sources, recovery can be done promptly.

All NBE information systems are subject to potential loss of data due to failure of hardware or software. It is the responsibility of relevant individuals to regularly make backup copies of essential data and store it in a safe location, remote from the main system. Computer media should be stored securely.

## 12. .Disciplinary Process

All users, including any third parties with access to NBE's information or computing systems, must comply with this Information Governance Policy as well as all other related Information Technology (IT) policies including the social media policy. This requirement is included in the conditions for staff, volunteers and Executive Officers and where appropriate compliance will be monitored.

After investigation if a user is found to have violated NBE's Information Governance Policy and/or procedures, they may be disciplined in line with the relevant disciplinary policy and potentially subject to legal proceedings. Other sanctions may include temporary suspension or withdrawal of access to member forums and / or social media sites.

## 13. Third Party Contractors

NBE is required to ensure confidential information is protected from inappropriate disclosure and must be processed lawfully. .

In order for NBE to comply with these duties they will ensure the third parties with whom they contract are subject to, and comply with, member and employee confidentiality, information security and data protection requirements. This will includes ensuring appropriate contract terms and or specific data sharing agreements are in place prior to any processing of personal information.

Where NBE has third parties gaining access to their assets, or the location of their assets,

© National Back Exchange 2018

contractors must ensure their staff are made aware of the Information Governance requirements and all applicable policies and procedures.

The growth of shared and partner working and the increased use of cloud based solutions has led to NBE outsourcing some information processing responsibilities. NBE will therefore ensure that information governance requirements and procedures included in all outsourcing contracts meet its business needs.

NBE will take all reasonable steps to ensure that the contractors and support organisations to whom personal information is disclosed comply with their contractual obligations to keep personal information secure and confidential.

Third party contractors and their sub-contractors and/or partner organisation are required to formally document their intention to indemnify NBE against breach of the information governance requirements in the performance of their contract.

Breach of information governance requirements by a third party contractor or their sub-contractor and/or partner organisation may result in immediate termination of the contract.

In addition to the contractual performance requirements above, NBE will also ensure that any third party contractor is aware of the possible impact of the Freedom of Information Act 2000 on the documentation connected with that contract.

## 14. Legal Compliance

NBE regards all personal information and confidential data as 'confidential information' and will only be shared with a restricted audience, except when and where legal obligations require otherwise.

NBE will establish and maintain policies for the controlled and appropriate sharing of member and or employee information with other partners or third parties, taking account of relevant legislation and legal obligations.

In order to meet the requirements of the membership, NBE will contact members for up to 12 months post expiry of membership to allow lapsed members to renew. There is an opportunity for new members to opt in to communication on other aspects related to moving and handling as part of the membership application process. Existing members are also encouraged to directly contact the admin team of any changes to their communication preferences following their initial application for membership.

## 15. Training

To maintain its information handling standards throughout the organisation, NBE will ensure that all employees and volunteers are provided with clear guidelines on their own obligations for confidentiality, data protection and information governance and security.

## 16. Audit Monitoring and Review

The Executive Committee will be responsible for implementing this policy and other

© National Back Exchange 2018

Information Governance related policies and procedures.

The review or creation of other Information Governance related policies and procedures will include mechanisms for monitoring compliance with this policy or other procedure standards.

This policy will be monitored and will be subject to an annual review. An early review may be warranted if one or more of the following occurs:

- As a result of regulatory / statutory changes or developments
- As a result of NBE policy changes or developments
- If a significant near miss or data breach occurs
- For any other relevant or compelling reason

All policies and procedures developed under this policy will be developed to allow compliance with the General Data Protection Regulation ('GDPR') which will be in force from May 2018. This policy will be reviewed and updated to fully reflect the GDPR requirements.

## 17. Version Control Information and History

| Date | Version no. | Status | Summary of changes | Consulting group / person | Changes made by |
|---|---|---|---|---|---|
| July 2018 | 1 | | New Policy | NBE Exec<br>Professional Affairs Committee | Professional Affairs Chair<br>Vice Chair |

© National Back Exchange 2018

# Risk assessment – Information Security

**July 2018**
**Review date July 2019**

**Organisation name: National Back Exchange**

| | |
|---|---|
| **Scope of risk assessment** | Requirement to demonstrate compliance with newly introduced GDPR regulation and Data Protection Act 2018. Management of personal information of members, conference delegates and trade database and old access member database |

| What are the hazards? | Who might be harmed and how? | What are you already doing? | Do you need to do anything else to manage this risk? | Action by whom? | Action by when? | Done |
|---|---|---|---|---|---|---|
| Loss of member data through computers being stolen or hacked into or office papers being stolen during a break in | Members personal information may be misused<br>Failure of business continuity due to lack of relevant data being available to support our members<br>Reputation of NBE | Burglar alarm for office<br>CCTV in car park at office<br>Computers password protected<br>Data backed up to external hard drive to ensure business continuity in response to potential data loss<br>Access to databases in line with requirements of the Data Protection Act 2018 i.e. limited to specified, explicit and legitimate purposes, minimising collection and storage of personal of data, ensuring security integrity and confidentiality of personal data, ensuring accuracy of personal data and enabling it to be erased or rectified, transparency, fairness and lawfulness in the handling and use of personal data | Source cloud based storage solution<br><br>Review current data held and ensure it complies with the timescales as outlined in appendix 2. | Admin team to present options to Exec for agreement | September 2018 | |
| Failure to comply with data protection legislation | Members personal information may be misused<br>Failure of business continuity due to lack of | Opt in for communications part of member application and renewal process<br><br>Facility to change communication | Inform members the opt in communication options and how to change communication preferences<br><br>Disseminate updated information re | Admin Team<br><br>Regional Officers | | |

© National Back Exchange 2018

| | | | | | | |
|---|---|---|---|---|---|---|
| | relevant data being available to support our members<br>Reputation of NBE | preferences at any time by communication to admin team<br><br>Updated information governances policy outlining how information is kept secure at national and affiliated group level | security of information to affiliated groups<br><br>Post updated policy on NBE website<br><br>Post information on social media forums informing members of updated policy | Communications Officer<br>PRO | | |

© National Back Exchange 2018

**Appendix 2**

## Retention of Documents Schedule

| Type of Record | Rationale for keeping it | Normal retention period | Action at end of retention period | Notes |
|---|---|---|---|---|
| Member personal information on member and conference database | Communication with membership | Life of organisation plus 6 years | Review and if no longer needed, destroy | Some members have gaps in their membership and keeping the records allows us to support our members to evidence their length of membership and their membership status at any given point in their career – this information may be needed to help support them in the event of claims / complaints against them |
| Trade database | Communication with trade partners | Life of organisation plus 6 years | Review and if no longer needed, destroy | |
| NBE policies and procedures | Historical record of systems in place at time | Life of organisation plus 6 years | Review and if no longer needed, destroy | |
| Internet site information | Historical record of information available at that time | | Review and if no longer needed, destroy | |
| Column – quarterly journal | Historical record of information available at that time | Electronic copy – lifetime of organisation plus 6 years | | |

© National Back Exchange 2018