DATA PROTECTION POLICY

The policy is created and approved by the board of directors.

ECO Action Network Eastbourne

CONTENTS

60 Rattle Road
Westham, Pevensey
East Sussex BN24 5DJ

hello@ecoactioneb.co.uk
https://ecoactioneb.co.uk

CONTEXT AND OVERVIEW

Introduction

Eastbourne ECO Action Network needs to gather and use certain information about individuals.

These can include members, customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures *Eastbourne ECO Action Network*:

- Complies with data protection law and follows good practice
- Protects the rights of staff, members, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 2018 describes how organisations — including *Eastbourne ECO Action Network* — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act imposes the General Data Protection Regulation (GDPR) underpinning six important principles.

1. Personal data processing must be lawful and fair
2. The purposes of processing must be specified, explicit and legitimate
3. Personal data must be adequate, relevant and not excessive
4. Personal data must be accurate and kept up to date
5. Personal data must be kept for no longer than is necessary
6. Personal data must be processed in a secure manner

RISKS AND RESPONSIBILITIES

Policy scope

This policy applies to:

- The head office of *Eastbourne ECO Action Network*
- All action groups of *Eastbourne ECO Action Network*
- All staff and volunteers of *Eastbourne ECO Action Network*
- All contractors, suppliers, facilitators and other people working on behalf of *Eastbourne ECO Action Network*

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Professional status of individuals
- Financial information for individuals

- Any other personal data retained by *Eastbourne ECO Action Network*

Data protection risks

This policy helps to protect *Eastbourne ECO Action Network* from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with *Eastbourne ECO Action Network* has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that *Eastbourne ECO Action Network* meets its legal obligations.
- The **Data Protection Officer** is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data *Eastbourne ECO Action Network* holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **Executive Director** is responsible for:
    - Ensuring all IT systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- The **Director of Communications** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees or volunteers can request it from their group curating director or the Data Protection Officer.
- *Eastbourne ECO Action Network* **will provide training** to all employees and volunteers to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees and volunteers **should request help** from their group curating director or the Data Protection Officer if they are unsure about any aspect of data protection.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or the Data Protection Officer.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees or volunteers should make sure paper and printouts are **not left where unauthorised people could see them**, ex. on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD, DVD or USB), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **not be saved directly** to unapproved laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

DATA USE

Personal data is of no value to *Eastbourne ECO Action Network* unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees or volunteers should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts. One of the way of securing data is save it to a password-protected file.
- Personal data should **never be shared with the third parties**, commercially or otherwise, unless on expressed agreement by the data owners.
- Employees or volunteers **should not save copies of personal data to their own computers** or access and update the central copy of any data.

DATA ACCURACY

The law requires *Eastbourne ECO Action Network* to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort *Eastbourne ECO Action Network* should put into ensuring its accuracy.

It is the responsibility of all employees and volunteers who work with data held by *Eastbourne ECO Action Network* to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Employees and volunteers should not create any unnecessary additional data sets.
- Employees and volunteers should **take every opportunity to ensure data is updated.** For instance, by regularly confirming group members' details.
- *Eastbourne ECO Action Network* will make it **easy for data subjects to update the information** *Eastbourne ECO Action Network* holds about them. For instance, via the company website or email.
- Data should be **updated as inaccuracies are discovered**. For instance, if a volunteer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Director of Communication's responsibility to ensure **marketing databases are checked against industry suppression files**.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by *Eastbourne ECO Action Network* are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at hello@ecoactioneb.co.uk. The Data Protection Officer can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The Data Protection Officer will aim to provide the relevant data within 14 days.

The Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, *Eastbourne ECO Action Network* will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

PROVIDING INFORMATION

Eastbourne ECO Action Network aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]