

The Bee Sanctuary Movement

Charity No: 1187263



Data Protection Policy

Context and overview

Key details

- Policy prepared by: Brian McGill [Treasurer]
- Approved by trustees on: 14-09-2021
- Policy became operational on: 14-09-2021
- Next review date: 06-04-2031

Introduction

The Bee Sanctuary Movement needs to gather and use certain information about individuals.

These can include Trustees, Volunteers, 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 The Bee Sanctuary Movement:

- Complies with data protection law and follow good practice

- Protects the rights of trustees, volunteers and employees
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The UK General Data Protection Regulations, including the Data Protection Act 2018 describes how organisations — including The Bee Sanctuary Movement— 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 is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- All Trustees, Volunteers and Employees of The Bee Sanctuary Movement
- All Contractors, Suppliers and other people working on behalf of The Bee Sanctuary Movement

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 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals

Data protection risks

This policy helps to protect The Bee Sanctuary Movement 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 The Bee Sanctuary Movement 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 Trustees are ultimately responsible for ensuring that The Bee Sanctuary Movement meets its legal obligations.

- The Data Protection Compliance Officer, Brian McGill, is responsible for:
 - Keeping other trustees 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 The Bee Sanctuary Movement 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.
 - Note: The Data Protection Compliance Officer is not the same as a Data Protection Officer as defined by the Information Commissioner's Office

Each Trustee, is responsible for:

- Ensuring all systems, services and equipment, under their control, used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software, under their control, is functioning properly.
- Evaluating any third-party services the trustee is considering using to store or process data. For instance, cloud computing services.

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 the Trustees.

- Trustees, Employees and Volunteers 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 the Trustees 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 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:

- Trustees, Employees and Volunteers should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be destroyed 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 or DVD), these should be kept securely when not being used.

- Data should only be stored on designated computers, and should only be uploaded to an approved cloud computing service.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the organisation's standard backup procedures.
- Data should never be saved directly to mobile devices like tablets or smartphones. Laptops are allowed provided they are password protected and kept in sight of the user
- All computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to The Bee Sanctuary Movement 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 should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Personal data should never be transferred outside of the European Economic Area.

Data accuracy

The law requires The Bee Sanctuary Movement 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 The Bee Sanctuary Movement should put into ensuring its accuracy.

It is the responsibility of all Trustees, Employees and Volunteers who work with data 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. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- The Bee Sanctuary Movement will make it easy for data subjects to update the information The Bee Sanctuary Movement holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by The Bee Sanctuary Movement 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 Compliance Officer: beesanctuary@outlook.com.

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

Currently the only data the organisation holds about individuals is stored in the financial records such as expenses forms and receipts. This data cannot be updated as it needs to be kept in its original form.

The Data Protection Compliance 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, The Bee Sanctuary Movement will disclose requested data. However, the Data Protection Compliance Officer will ensure the request is legitimate, seeking assistance from the trustees and from the company's legal advisers where necessary.

Providing information

The Bee Sanctuary Movement 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.

Last Revised - May 2023