Bexhill Heritage
Conservation, protection and improvement of the Bexhill-on-Sea built environment.

Bexhill Heritage Data Protection and Data Security Policy

This policy includes *Computer Use Procedures* attached as Appendix A.

1. Introduction

This data protection policy applies to Bexhill Heritage (hereafter described as 'the charity'), a small charity safeguarding the future of heritage assets in Bexhill-on-Sea.

Purpose

Members, officers and trustees of the charity must do their best to safeguard colleagues' and donors' personal data as if it were their own.

In seeking to respect and protect personal data we will use processes that, as a minimum, are fully consistent with the relevant national legislation (Data Protection Act 1988 and the General Data Protection Regulations [GDPR] 2018), the common-law duty of confidentiality and the requirements of relevant regulators, particularly the Office of the Information Commissioner (ICO).

The purpose of this policy is to ensure that all officers and trustees:

- are fully aware of what constitutes personal data
- act in ways that fully respect other people's legal and moral rights to have their data protected
- retain personal data only where it is necessary to:
    - identify and communicate with members
    - contact members' family or friends in the event of an emergency
    - protect children or vulnerable adults
    - record aspects of members', officers' or trustees' service that will contribute to performance enhancement or review
    - record members' consent for reclaiming Gift Aid on their donations or membership subscriptions

- record employment data necessary for an employer to meet their statutory responsibilities
- contact donors or potential donors.
- record a complaint

- fully respect confidentiality in ways that are consistent with peoples' rights to privacy under current legislation
- gain members' informed, written consent when personal data is recorded and retained except in exceptional cases where an adult is unable to make decisions for themselves. In such cases we will deal with their nominated representative
- process data fairly and lawfully in accordance with the rights of 'data subjects'
- store data securely so that it can be accessed only by authorised members of the charity
- ensure that organisational security measures for stored data are in place and support such measures
- destroy data immediately after there is no further need to retain it
- understand that it is unacceptable to retain personal data for research or administrative convenience
- and finally …. understand that information governance helps the charity to manage the risks associated with obtaining, holding or storing, using and sharing, and disposing of information.

1.1 <u>What is data? The branch as a 'data controller'.</u>

Data includes any automated or non-automated records that are organised in a way which allows ready access to information about individuals.

The charity is a 'data controller' under the GDPR 2018 (see below) but is currently exempted from registration with the Information Commissioners Office (ICO). Nevertheless, the charity adheres to the principles of the General Data Protection Regulations and its officers understand best practice for managing information

1.2 What is personal data under the GDPR 2018?

- Any information relating to a living individual relating to his or her private, professional or public life that identifies them **or** could identify them if combined with other information in the possession of, or likely to come into the possession of, the charity. Examples – name and contact number of member or donor, home address, post code, email address, etc.
- Data that links to, relates to or is about a living individual. Examples – membership record, donation record, tax status, video recordings and photographs.
- Data used to inform or influence actions or decisions affecting an identifiable individual. Example – a note of the outcomes of a charity project.

For more information refer to guidance from the Information Commissioner's Office (ICO) UK GDPR guidance and resources | ICO

1.4 What are peoples' data protection rights in law?

Everyone enjoys the same data protection rights under the 2018 General Data Protection Regulations.

All individuals about whom the charity holds data have the following legal rights:

a. to be informed about and give explicit consent to the collection, organisation, use and arrangements for the deletion of personal data

b. to have contact details of whom to contact at Bexhill Heritage to make an enquiry or complaint

c. to object to processing that is likely to cause or is causing damage or distress

d. to access a copy of personal data

e. to have personal data rectified, blocked, erased or destroyed; and

f. to claim compensation for damages caused by a breach of the 2018 GDPR.

For more information refer to guidance from the Information Commissioner's Office (ICO)

A guide to individual rights | ICO

1.5 What are the legal circumstances where the charity can process (collect, organise, store and transfer) personal data?

a. the member, employee or donor has given consent to the processing of their personal data for one or more specific purposes

b. processing is necessary for the performance of a contract or project to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract e.g. obtaining references

c. processing is necessary for compliance with a legal obligation to which the controller is subject e.g. cooperation with relevant public authorities

d. processing is necessary in order to protect the vital interests of the data subject or of another person

e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

1.6 The charity's approach data protection and the role of its data protection officer

The charity seeks to be fully respectful of people's personal data and to comply fully the General Data Protection Regulations, 2018.

The charity is exempted from appointing a data protection officer (DPO) and trustees have decided not to make a specific appointment at this time. Although the charity does not need to appoint a DPO, trustees recognise that it's important to have someone in the charity who is responsible for data protection. Currently that person is the treasurer. The treasurer, supported by the trustees, will ensure that privacy is a set at 'a high level by default' and that technical and procedural measures are in place to ensure that data processing, throughout the whole processing lifecycle, complies with the regulations. The treasurer will ensure that personal data is only processed when necessary for each specific purpose and will maintain records of processing activities.

2. Guidelines

2.1 Data relating to members

2.1.1 Seeking consents and providing information about data processing

The GDPR specifies the information that the charity is required by law to give to members. This is set out in the chart that follows. This must be done when a member joins the charity by the treasurer. In the case of employees, this must be done on appointment. In this way, members and employees should be clear about the nature of the personal data held by the charity and the reasons it is held. Members and employees must give their written permission for personal data to be held for **each of** these purposes.

Information given by the charity to members, registered donors and employees
1. The existence of each of data subject's rights (a copy of the charity's policy and guidelines)
2. Identity and contact details of the branch treasurer (responsible for data protection)
3. Details of the personal data to be collected
4. Purpose of the storage and processing of their personal data and the lawful basis for the processing including whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
5. The legitimate interests of the charity (data controller) in relation to 3 and 4 above
6. Retention period for personal data and criteria used to determine the retention period
7. The right to withdraw consent at any time, where relevant
8. The right to lodge a complaint with the Information Commissioners Office (ICO)

2.1.2 Circumstances where anonymised data can be used within the charity

Anonymised data can be used by officers and trustees to inform forward planning, recruitment, retention and strategies to engage members in the charity's work.

2.1.3 Processing, storing and destroying data

The charity processes personal data about members for the following purposes:

- keeping in touch with members and issuing information
- sending reminders about membership renewal

- identifying members who may have an interest or capacity to join or lead a project
- coordinating criminal record disclosures
- communication purposes between members (This includes name and, email or phone number but not postal address.)
- member expenses
- protecting the charity's legal responsibilities with respect to such issues as health and safety, equalities, safeguarding and reclaiming Gift Aid (where members and donors have given their consent).

Personal data about members is stored on restricted computer files. Access to the restricted files is enabled for the chairman, treasurer, the officer responsible for member retention and recruitment, and the officer responsible for IT support.

Personal data relating to volunteers is not recorded in official records such as minutes of member, committee or trustee meetings.

Data relating to members and donors will be destroyed 30 days after they cease to become members or donors unless they have given their consent for the charity to reclaim Gift Aid on their subscription or donation when records will be destroyed once the Gift Aid claim has been processed by Her Majesty's Revenue and Customs (HMRC). This will be a maximum of 24 months after they cease being a member. Should the charity be 'wound up' all membership records will be destroyed 30 days after the winding up resolution has been passed.

Personal data relating to members or employees will not be passed to other organisations without the explicit written consent of the individual or except in response to legitimate legal enquires by the relevant authorities.

2.3 <u>Data relating to donations, including 'gift aid'</u>

2.3.1 Seeking consents and providing information about data processing

For donations with a value of £100 or more, or direct debits, donors or third parties acting on behalf of donors must be advised that their personal contact details and the nature of the donation will be recorded. In the case of direct debits, this will include bank details.

Donors will be asked for their consent to 'Gift Aid' their donation.

Donors will be asked for their consent for the charity to publicly recognise their donation. Should this consent be withheld, the source of the donation will remain confidential to the chair and the branch officer responsible for fund raising.

2.3.2 Processing, storing and destroying data

Personal records relating to donors will be held in a secure filing system within the branch for access by the chairman, treasurer and the branch officer responsible for fund raising only.

Such personal records will be destroyed after 24 months.

No personal data relating to donors or the organisations they represent will be passed to other organisations without their explicit, written consent.

3. Subject access requests

Members and donors have the legal right to know what information the charity holds on them, what the charity does with it and who it may be shared with. This is known as a subject access request.

Data subjects can ask to be supplied with copies of both paper and computer records and related information.

Appropriate third parties can act on behalf of a vulnerable person. In addition, advocates can act on an enquirer's behalf. In these cases, the branch secretary must satisfy themselves that the third party making the request has the individual's permission to act on their behalf. It is the third party's responsibility to provide this evidence, which could be a written authority to make the request, or a power of attorney.

Data subjects must provide proof of identity including full name and postal address. Such requests must be made in writing and the charity must respond within 40 calendar days by secure post.

4. The Information Commissioners Office (ICO)

The ICO is the UK's independent body to uphold information rights. Its role is to:

- monitor the register of data controllers
- deal with concerns about information handling
- take action to enforce the current legislation.

Bexhill Heritage is an independent charitable organisation but is exempt from registering as a data controller with the Information Commissioner's Office (ICO).

5. Information security

Information security is everyone's responsibility. All members will:

- shred informal notes as soon as possible
- change their password as directed
- report any lost or missing keys to the chair
- not load personal data on to personal electronic devices
- never discuss confidential information outside the charity or share it on social media
- never share passwords.

To ensure a reasonable level on information security the treasurer will check that the data retention schedule is adhered to.

The officer responsible for maintaining the central data file will ensure that:

- the charity's computer is used only to support the charity's legitimate business and is kept securely
- passwords are changed at least every 12 months and are suitably robust
- the charity's equipment is disposed of in a way that ensures the confidentiality of records it may contain.

6. Training

The charity is responsible for ensuring that all officers are trained in and understand the basic principles of data protection.

7. CCTV

Although there is a CCTV warning notice in the Bandstand, a building leased by the charity, the Charity does not operate this video surveillance system. The camera focuses on the external perimeter of the building and that of the tea chalet opposite. The leaseholder of the tea chalet operates the CCTV system.

8. Questions and comments

Questions, observations about the policy and suggested amendments should be sent to the charity's chair.

9. Reporting data incidents / whistleblowing

Every member has shared responsibility for the effective implementation of this policy. If a member loses personal data through theft or human error, they will report this as soon as possible to the chairman. If a member believes that a password may have been compromised, they should change this immediately and inform the chair.

Any member who becomes aware of a minor breach of this policy such as failure to destroy informal notes, should bring it to the attention of the transgressor so that appropriate remedial action can be taken.

Any member who becomes aware of persistent minor breaches of this policy or a major breach must report the incident to the treasurer or chair. However, if both treasurer and chair are involved in the data breach, members should report the incident to one of the other trustees. Reporting should be done in writing but may be done anonymously. Concerned members also have the right to contact the ICO with their concerns.

If the treasurer and / or the chair become aware of any breach of data security, they must notify the individuals concerned and the ICO within 72 hours.

10. Monitoring and review

The charity has audited its operations and considered how each area is compliant with data protection legislation. All changes to services and processes are assessed for data protection implications.

The charity's treasurer has oversight of data protection and will report to the trustees. The treasurer will ensure that the charity follows the Caldicott Principles which underpin legislation such as the GDPR:

1. Any use of personal confidential data (PCD) must be justified.
2. Such data must not be accessed unless it is absolutely necessary.
3. Only the minimum amount of data should be accessed.
4. Data should only be accessed on a 'need-to-know' basis.
5. Everyone should be aware of their responsibilities for protecting personal data.
6. Everyone should understand and comply with the law.

7. The duty to share information, for example in a safeguarding situation, can be as important as the duty to protect confidentiality.

The trustees will review and update this policy every two years.

Appendix A: Computer use procedures and related data protection processes

Use of the charity's computers

1. The charity's computers are provided for the service and admin purposes and should not be used for personal use as this could be viewed as misconduct.
2. Using one of the charity's computers to view or download offensive material from the internet, or causing harassment through the use of e-mail, could amount to serious misconduct.
3. To ensure compliance with data protection and other legislation the charity undertakes the following:
    a. has a named IT support officer and only this designated IT support officer may do the following:
        i. change any of the settings on any of the charity's computers
        ii. load or delete any software or files to the charity's computers
        iii. run any diagnostic tools on any of the charity's computers.
    b. all the charity's computers have firewalls and virus checker installed which includes anti-spyware software
    c. unsupported operating systems are not installed or used on branch computers.
4. The charity's computers and IT systems must only be used for designated purposes and in accordance with official policies and guidance. The charity is responsible for ensuring that officers know which systems can be accessed.

Policy reviewed: January 2025

Next review date: January 2027