



## **General Data Protection Regulation**

### **Purpose of the policy and background to the GDPR**

This policy explains to trustees, members, staff and the public about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy explains the duties and responsibilities of the Trust and it identifies the means by which the Trust will meet its obligations.

### **Reasons for holding personal protected and secured information**

The Trust may hold information about individuals in order to manage its affairs and its assets in accordance with its Constitution and for no other reason. Such information is needed to communicate with members and potential members of Trust, its Trustees, suppliers and contractors, organisations with which it involved or with whom it may become involved and in connection with individuals hiring or leasing the Trust's properties or interested is so doing either in their own right or as representatives of third party organisations. Such information held will not be divulged to other parties without the specific agreement of the individual concerned and the information by whomsoever it is accessible will at all times be secured whether electronically by means of protected passwords or if in printed form retained in locked cabinets or drawers.

### **Identifying the roles and minimising risk**

GDPR requires that everyone within the Trust must understand the implications of GDPR and that roles and duties must be assigned. The Trust is the data controller. It is the Clerk's duty to undertake an information audit and to manage the information collected by the Trust, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information.

GDPR requires continued care by everyone within the Trust, trustees and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the Trust facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as medium risk to the Trust (both financially and reputationally) and one which must be included in the Risk Management Policy of the Trust. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the Trust undertaking training in data protection awareness.

## **Data breaches**

Personal data breaches should be reported to the Clerk for investigation. The Clerk will conduct this with the support of the Trust. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Clerk will also have to notify those concerned directly.

It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Trust, for example the discussion of internal Trust matters on social media sites could result in reputational damage for the Trust and to individuals.

## **Privacy Notices**

Being transparent and providing accessible information to individuals about how the Trust uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a Trust does with their personal information. A privacy notice will contain the name and contact details of the Clerk, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the Trust. The Trust will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

## **Information Audit**

The DPO must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the Trust undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

## **Individuals' Rights**

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, then the Clerk must respond to this request within a month. The Clerk has the delegated authority from the Trust to delete information.

If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the Trust's Freedom of Information Publication Scheme. The Trust will be informed of such requests.

## **Summary**

The main actions arising from this policy are:

- A copy of this policy will be available on the Trust's website. The policy will be considered as a core policy for the Trust.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- Data Protection will be included on the Trust's Risk Management Policy.
- The Trust will manage the process.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

All employees, volunteers and trustees are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Trust.



## **GDPR - Privacy Notice**

Personal data is any information about a living individual which allows them to be identified from data, for example, name, photograph, video, email address, address. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (GDPR).

Benenden Village Trust takes the protection of your data seriously. Our aim is to provide a personalised and valuable service whilst safeguarding our users' privacy. Collecting some personal information is necessary if we are to satisfy the expectations and requirements of our users and we have set out below what we will do with your personal information. BVT complies with its obligations under the GDPR by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data. Responsibility for data management is delegated by the Trust to the Clerk.

### **Visitors to this web site**

When someone visits this website, we or the website administrators use a third party service, to collect standard internet log information and details of visitor behaviour patterns. We and they do this to find out things such as the number of visitors to the various parts of the site. This information is only processed by us in a way which does not identify anyone. If we do want to collect personally identifiable information through our website, we will say so in advance. We will make it clear when we collect personal information and will explain what we intend to do with it.

### **Security and Performance**

We use a third party service to help maintain the security and performance of our website. To deliver this service it processes the IP addresses of visitors to the site.

### **Links to other websites**

This privacy notice does not cover the links within this site linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

### **Use of Cookies**

This site uses cookies to maintain and keep track of users' preferences and authenticated sessions, to identify technical issues, user trends and effectiveness of campaigns, and to monitor and improve the overall performance.

## **Disclosure of personal information**

We collect contact details via the web site for the purposes of providing a service to existing and potential correspondents and residents. We will never disclose personal details without the consent of the owner unless required to by law. Details are only held for as long as is necessary for Trust business, normally not more than 7 years.

## **Access to personal information**

Individuals can find out if we hold any personal information by making a 'subject access request' under the General Data Protection Regulations. If we do hold information about you we will:

- give you a description of it;
- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

To exercise all relevant rights, queries or complaints in the first instance contact the Clerk via email [bvtclerk@gmail.com](mailto:bvtclerk@gmail.com) or by post to Benenden Village Trust, Community Office, Benenden Village Hall, Benenden, Kent, TN17 4DE. We will normally respond within 20 days.