# Data Protection Policy

## **INTRODUCTION**

Bonny Downs Community Association (BDCA) is committed to ensuring the secure and safe management of the personal data it holds. Staff members have a responsibility to ensure compliance with this policy, and to manage individuals’ data in accordance with the procedures outlined and documentation referred to in this policy.

BDCA needs to gather and use certain information about individuals. These can include service users, employees, trustees, volunteers, donors, supporters, job applicants and other individuals that BDCA has a relationship with. BDCA manages data from a variety of sources.

This Policy sets out BDCA’s duties in processing that information, and the purpose of this policy is to set out the procedures for the management of such data.

## **LEGISLATION**

It is a legal requirement that BDCA process data correctly: BDCA must collect, handle and store personal data in accordance with:

* + The General Data Protection Regulation (EU) 2016/679 (“the GDPR”);
	+ The Privacy and Electronic Communications Regulations 2018; and
	+ The Data Protection Act 2018.

## **DATA**

BDCA holds a variety of data relating to individuals (also referred to as data subjects) which is known as personal data. The personal data held and processed by BDCA is detailed within its privacy notices.

“Personal Data” is that from which a living individual can be identified by reasonable means either by that data alone, or in conjunction with other data held by BDCA or publicly available.

BDCA may also hold personal data that is sensitive in nature (i.e. relates to or reveals a data subject’s racial or ethnic origin, religious beliefs, political opinions, trade union membership, genetics, biometrics, health, sex life or sexual orientation). This is “Special Category Data” (sometimes known as “Sensitive Personal Data”).

## **PROCESSING OF PERSONAL DATA**

Processing of personal data includes the collection, storage, retention and disposal of that data. BDCA is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

* Processing occurs with the consent of the data subject;
* Processing is necessary for the performance of a contract between BDCA and the data subject or for entering into a contract with the data subject;
* Processing is necessary for BDCA’s compliance with a legal obligation;
* Processing is necessary to protect the vital interests of the data subject or another person;
* Processing is necessary for the performance of a task carried out in the public interest or in the exercise of BDCA’s official authority; or
* Processing is necessary for the purposes of legitimate interests.

## **PRIVACY NOTICES**

BDCA will provide privacy notices to all data subjects whose personal data it holds. Privacy notices are provided to data subjects from the outset of processing their personal data.

## **CONSENT**

Consent may be used as a ground for processing personal data by BDCA. It will only normally be used by BDCA where no other lawful basis for processing is available. Where consent is relied upon as a lawful basis for processing personal data, the consent should be informed, freely given, specific, current, and evidenced. A record of consent will be kept and consent should be renewed at least every 2 years.

## **PROCESSING OF SPECIAL CATEGORY PERSONAL DATA**

In the event that BDCA processes Special Category Personal Data, it must do so in accordance with one of the following grounds of processing:

* The data subject has given explicit consent to the processing of this data for a specified purpose;
* Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
* Processing is necessary to protect the vital interest of the data subject or of another person where the data subject is incapable of giving consent;
* Processing is carried out as part of BDCA’s legitimate activities, relates only to individuals with whom it has regular contact, and the personal data is not disclosed beyond BDCA without data subjects’ explicit consent;
* Processing relates to data made public by the data subject;
* Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity;
* Processing is necessary for reasons of substantial public interest;
* Processing is necessary for reasons of preventative or occupational medicine, public interest in the area of public health, or public interest in the areas of historic or scientific research.

BDCA will refer to Article 9 of GDPR and Schedule 1 (parts 1 &2) of the Data Protection Act 2018 when establishing conditions for processing Special Category data.

## **DATA SHARING**

BDCA only shares data with third parties in order that its day-to-day activities are carried out and contractual agreements are met in accordance with BDCA’s relevant policies and procedures.

Personal data may be shared within BDCA and with some third parties who act as data processors for BDCA. BDCA does not normally share data with other data controllers. Where this is necessary (for example, where BDCA is fulfilling a contractual service where it is required to submit personal data as part of its reporting, or to refer a service user to another organisation) BDCA will obtain prior consent from the data subject.

Where BDCA shares personal data with a third party organisation, it shall require the third party to provide evidence of compliance with data protection legislation.

BDCA will take steps to ensure the secure transfer of personal data:

* We will only transfer personal data to other organisations where it is necessary to do so, where the appropriate consent has been given, and where we are satisfied that the recipient has appropriate measures in place to comply with data protection law.
* When transferring data electronically, we will use password protected documents/storage devices to ensure that the data remains secure in transit. Passwords will be given separately (eg: in a separate email, or via telephone).
* Where practical, personal data will be handed over in person (eg: at a case conference).

## **DATA PROCESSORS**

A data processor is a third party entity that processes personal data on behalf of BDCA (e.g. payroll, database host, credit card payment processor).

A data processor must comply with Data Protection laws. BDCA’s data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities, notify BDCA if a data breach is suffered, and undertake not to use data held by BDCA for any purpose besides those directed by BDCA as data controller.

If a data processor wishes to sub-contract their processing, BDCA’s prior written must be obtained. The data processor will be liable in full for the data protection breaches of their sub-contractors.

## **DATA STORAGE AND SECURITY**

All Personal Data held by BDCA must be stored securely, whether electronically or in paper format.

1. Paper Storage

If personal data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. When the Personal Data is no longer required it must be disposed of securely, normally by shredding, to ensure it can no longer be linked to an individual.

1. Electronic Storage

Personal data stored electronically must also be protected from unauthorised use and access. If personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal data should only be stored on designated drives or servers (BDCA’s shared company drive/local server and Upshot database). When personal data is stored on mobile devices, these devices are to be password protected and stored securely when not in use.

## **BREACHES**

A data breach can occur at any point when handling personal data and BDCA has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects require to be reported externally.

1. Internal Reporting

BDCA takes the security of data very seriously and in the event of a breach will take the following steps:

* + When a breach or potential breach is discovered, a member of BDCA’s Strategy & Support Team must be notified immediately.
	+ The Strategy & Support Team will then investigate (i) the nature and extent of the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
	+ BDCA will seek to contain the breach at the earliest opportunity;
	+ The Strategy & Support Team will consider whether the breach is one which should be reported to the Information Commissioner’s Office (ICO) and data subjects affected and take the necessary steps to do so;
1. Reporting to the ICO

BDCA is required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the ICO within 72 hours of the breach occurring. BDCA must also consider whether it is appropriate to notify those data subjects affected by the breach.

## **DATA PROTECTION OFFICER**

BDCA has not appointed a Data Protection Officer, but may seek advice from a suitably qualified individual where appropriate. The CEO of BDCA has overarching responsibility and oversight of compliance by BDCA with data protection laws, and has delegated day-to-day responsibility to the Operations Manager. Any data protection issues can be raised by contacting info@bonnydowns.org.

The CEO is responsible for:

* Monitoring BDCA’s compliance with Data Protection laws and this Policy;
* Co-operating with and serving as BDCA’s contact for discussions with the ICO;
* Reporting breaches or suspected breaches to the ICO and data subjects where appropriate.

## **DATA SUBJECT RIGHTS**

Under GDPR, individuals have the following rights:

* Right to be informed
* Right of access
* Right to rectification
* Right to erasure (right to be forgotten)
* Right to restrict processing
* Right to data portability
* Right to object (to processing for direct marketing; scientific/historical research & statistics; or the performance of a legal task or BDCA’s legitimate interests)
* Right not to be subject to automated decision-making including profiling.

Right to be informed

BDCA will inform individuals of their rights at the point at which they share their data. In addition to their rights, BDCA will inform individuals about how we will use their data, how long we will retain it for, and the legal basis/bases for processing their data. BDCA will do this by providing an appropriate privacy notice.

Right of access

BDCA’s procedure for subject access requests is set out below.

Right to rectification

BDCA will make every effort to ensure the accuracy of data held on individuals. Where inaccuracies come to our attention, we will correct these at the earliest opportunity.

Right to erasure

Where an individual requests that BDCA erases some or all of their personal data, we will log and respond to this request without undue delay and normally within one month of receipt. Where this information is held in our database, we will remove any identifying information from the records through redaction or anonymization.

Right to restrict processing

Where an individual requests that BDCA restricts processing, we will log and respond to this request without undue delay and normally within one month of receipt. We will work with our data processors to determine effective systems for restricting processing on a case-by-case basis. We will inform individuals concerned before lifting a restriction on processing.

Right to data portability

Where an individual wishes to copy or transfer the data that BDCA holds about them to another entity, we will log and respond to this request without undue delay and within one month of receipt. Where the request is complex, this may be extended to two months and we will inform the individual and explain why the extension is necessary within one month of the request. We will aim to comply with the request when this right applies, but also where the right does not apply but it is appropriate to do so. Data to be transferred will normally be provided as an encrypted or password-protected csv file.

Right to object

Where an individual objects to BDCA using their personal data to undertake direct marketing, we must stop immediately. If the objection to BDCA processing personal data for other purposes, we will seek guidance from the ICO or a Data Protection Officer and comply with individual’s request where appropriate.

Right not to be subject to automated decision-making

BDCA does not currently use automated decision-making.

## **SUBJECT ACCESS REQUEST**

Individuals have a right to access their personal data and any requests to do so (whether verbally or in writing) will be treated as subject access requests.

Upon receiving a subject access request, the following procedure will be followed:

* Staff receiving a subject access request will alert the Senior Management Team at the earliest opportunity, who will respond to the request or provide appropriate support to the staff member responding to the request.
* The date, individual making the request and nature of the request will be recorded.
* The request will be acknowledged at the earliest opportunity.
* We will check which format the individual would prefer to receive their data in and comply with their preference where possible.
* Where there is any doubt, the identity of the individual making the subject access request will be verified (for example, we may request photographic ID before releasing the data). If the request is made via a third party, we will require verification that the third party is authorised to act on the individual’s behalf before releasing the data. If we need to verify legitimacy of a request, we will contact the individual or party making the request at the earliest opportunity.
* The request will be responded to within 28 days of receiving it.
* If the request is complex, we may extend the response time by a further 2 months. We will write to the individual explaining the reasons for this within 28 days of receiving the subject access request.
* In addition to the data requested in the agreed format, we will provide a copy of the appropriate privacy notice and an explanatory note where it would be difficult for the individual to make sense of the data otherwise.
* No fee will be charged for subject access requests, unless a request is manifestly unfounded or excessive.
* Where a request is manifestly unfounded or excessive, BDCA reserves the right to refuse or to charge a reasonable fee. We will write to the individual within 28 days of receiving the request explaining our reasons for refusing or charging, and advising them of their right to complain to the ICO or to seek judicial remedy.
* In the case of children, subject access rights reside with the child, not the adult with parental responsibility, although in the case of very young children a parent may reasonably exercise these rights on the child’s behalf. Once a child is mature enough to understand (in broad terms) what it is to make a subject access request, then any information requested should be given to the child, not the adult with parental responsibility. There is no prescribed age for this and therefore BDCA will deal with child subject access requests on a case-by-case basis, with reference to ICO guidance, and taking advice from a DPO if appropriate.
* Wherever possible, data pertaining to an individual making a subject access request will be isolated from data about other people. However, where this is impossible, BDCA will refuse to comply with the request unless:
	+ the other individual has consented to the disclosure; or
	+ it is reasonable to comply with the request without that individual’s consent.

BDCA will deal with such issues on a case-by-case basis, with reference to ICO guidance, and taking advice from a DPO if appropriate.

## **PRIVACY IMPACT ASSESSMENTS (“PIAS”)**

These are a means of assisting BDCA in identifying and reducing the risks that our operations have on personal privacy of data subjects.

BDCA shall:

1. Carry out a PIA before undertaking a new project or processing activity which poses a “high risk” to an individual’s privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and
2. In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.
3. BDCA will consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The CEO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they are required to notify the CEO within five (5) working days.

## **ARCHIVING, RETENTION AND DESTRUCTION OF DATA**

BDCA cannot store and retain personal data indefinitely. It must ensure that personal data is only retained for the period necessary. BDCA shall ensure that all personal data is archived and destroyed in accordance with the periods specified within the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ser | Data Description | Retention Period | Start of Period | Relevant Provision/Reason |
| 1 | Beneficiary personal data | Whilst a member | On Joining | To provide contact and enable support |
| 2 | Beneficiary personal data | 3 months | On request to leave | To allow a reasonable time for a change of mind |
| 3 | Beneficiary financial data | 6 years | End of financial year the payment was made | Charities Act 2011 Section 131. Charities and Trustee Investment (Scotland) Act 2005 Section 44 |
| 4 | Staff Personal Data – Personal files, including training records and notes | 6 years | Start of employment on an ongoing basis | To cover the time for civil legal action claims |
| 5 | Staff Financial Records- Payroll, Income Tax and pension information | 6 Years | End of financial year the payment was made | Charities Act 2011 Section 131. Charities and Trustee Investment (Scotland) Act 2005 Section 44 |
| 6 | Documents proving the right to work in the UK | 2 years | On leaving employment | Immigration Act 2016 |
| 7 | Trustee personal data | 10 years | Rolling basis | Charities Act 2011 – Board Meeting Minutes |
| 8 | Contact Information – Patrons Volunteers/ Supporters | As long as a Patron/Volunteer/Supporter | On agreeing to become Patron/Volunteer/ Supporter | To enable contact and provide information or for 6 Years if any financial transactions have taken place. |