Data Protection Policy

Policy information	
Organisation	Great Bowden Recital Trust
Scope of policy	Great Bowden Recital Trust
Policy operational date	01.07.2009
Policy prepared by	Anne Brown
Date approved by Board/ Management Committee	This policy was approved by the Trustees on the 29th day of October 2009
Policy review date	01.07.2012

Introduction	
Purpose of policy	The purpose of this policy is to comply with the law, follow good practice and to protect the organisation.
Brief introduction to Data Protection Act 1998	You must comply with the Act if you process personal data (being data which relates to a living individual who can be identified either from those data, or from those data and other information which is in our possession).
Data Protection Principles	There are 8 Data protection Principles which are:- 1 Fair and Lawful processing 2 Processing for limited processes 3 Data should be adequate, relevant and not excessive 4 Data must be accurate and up to date 5 Data must not be kept longer than is necessary 6 Data must be processed in line with subjects' rights 7 Data must be kept secure 8 Data must not be transferred to other countries without adequate protection
Personal data	This would include name, address, email address, telephone number, date of birth and information about the individual from which the individual can be identified. If the person cannot be identified by the piece of data, then it is not personal data.
Policy statement	This could include a commitment to: comply with both the law and good practice respect individuals' rights be open and honest with individuals whose data is held
Key risks	Information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information.

Responsibilities	
Trustees	They have overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	This will be Elizabeth Anne Brown. Their responsibilities include: Briefing the trustees on their Data Protection responsibilities Reviewing Data Protection and related policies Notification (see notes) Handling subject access requests Approving unusual or controversial disclosures of personal data Approving contracts with Data Processors (see notes)
Specific other staff	Andrew Cartwright will be responsible for electronic security and for including Data-Protection-related statements on publicity materials, letters etc
Staff & volunteers	All staff and volunteers should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'staff' is used, this includes both paid staff and volunteers.)
Confidentiality	
Scope	Confidentiality applies to a much wider range of information than Data Protection. Some of the things that are likely to be confidential, but may well not be subject to Data Protection, include: Information about the Trust (and its plans or finances, for example) Information about other organisations, since Data Protection only applies to information about individuals Information which is not recorded, either on paper or electronically Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act
Understanding of confidentiality	Access to confidential information will be on a "need to know" basis. Information regarding illegal behaviour and affecting the health of children either mentally or physically will be shared with the appropriate legal guardian or appropriate authorities.
Communication with Data Subjects	All information held will be kept confidential but will be shared with responsible adults on a need to know basis only
Authorisation for disclosures not directly related to the reason why data is held	For a disclosure which is at the instigation of or in the interests of the data subject, then consent of the data subject will be the only authorisation required. Consent should be recorded. For a disclosure made in the course of official investigations, such as a criminal investigation, then the Data Protection Officer or the Chairman can make the decision to authorise the disclosure.

Security	
Scope	Security is about ensuring that confidential information is kept secure.
Setting security levels	All data and other information held by the Trust must be kept secure.
Security measures	Information held on computer should be password protected and information stored in paper form should be kept in files or folders and stored in an appropriate manner.
Continuity	Data held on computer should be backed up once every week
Specific risks	None.

Data recording and storage	
Accuracy	When collecting any personal data, care should be taken to ensure that it is correctly recorded and in case of doubt double checked with the data subject
Updating	No regular updating will be initiated by the Trustees
Storage	Storage of names and addresses will be both in electronic and written format
Retention periods	Every three years we will review the data we are holding and any data which we no longer need to retain will be destroyed.
Archiving	Electronic data will be deleted and paper data will be shredded.

Transparency	
Commitment	We will inform data subjects of the purpose for collecting the data and that we will not disclose information about them without their consent
Procedure	We will inform potential data subjects of our commitment with a statement on our website. Data subjects will be added to the Trust mailing list for future events only organised by Great Bowden Recital Trust. Such information will not be shared with any third party

Direct marketing	
Underlying principles	Although the Act does not define direct marketing clearly enough to be certain whether it incorporates many of the activities of voluntary organisations, good practice suggests that most unsolicited direct contact with individuals should be treated as marketing. This would include seeking donations, marketing goods and services, promoting sponsored events, raffles, etc.
Opting out	Data Subjects have the right to require their data not to be used for marketing. We will provide easy access to opting out of future marketing at the earliest opportunity.

Volunteer training & acceptance of responsibilities	
Documentation	All our procedures relating to Data Protection are contained in this policy document.
Other related policies	There are no related policies.
Induction	All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures.
Procedure for staff signifying acceptance of policy	Staff will be required to read and sign a copy of this Policy to signify their acceptance of it.

Appendix I

Data Controller

The Data Controller is the legal 'person' responsible for complying with the Data Protection Act. It will almost always be the organisation, not an individual staff member or volunteer. Separate organisations (for example a charity and its trading company) are separate Data Controllers. Where organisations work in close partnership it may not be easy to identify the Data Controller. If in doubt, seek guidance from the Information Commissioner.

Data Processor

When work is outsourced, which involves the contracting organisation in having access to personal data, there must be a suitable written contract in place, paying particular attention to security. The Data Controller remains responsible for any breach of Data Protection brought about by the Data Processor.

Fair processing conditions

Schedule 2 of the Data Protection Act lays down six conditions, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

- With consent of the Data Subject
- If it is necessary for a contract involving the Data Subject
- To meet a legal obligation
- To protect the Data Subject's 'vital interests'
- In connection with government or other public functions
- In the Data Controller's 'legitimate interests' provided the Data Subject's interests are not infringed

Notification

All Data Controllers have to consider whether they are exempt from Notification. If they are not exempt, they have to Notify. This means completing a form for the Information Commissioner, and paying a fee of £35 a year. The Notification form covers:

- The purposes for which personal data is held (from a standard list) and for each purpose (again from standard lists):
- The types of Data Subject about whom data is held
- The types of information that are held
- The types of disclosure that are made
- Any transfers abroad

There is probably no need to mention the details of the organisation's Notification in the policy. The Notification entry has to be reviewed each year, and may have to change if the organisation changes its processing in significant ways.

Subject access

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request (including the fee, if required), the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld. This includes some third party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)

I confirm that I have read and will be bound by this Data Protection Policy

Signed……..

Full name……

Date……..

Signed……..

Full name……

Date……..

Signed……..

Full name……

Date……..

Signed……..

Full name……

Date……..

Signed……..

Full name……

Date……..

Signed……..

Full name……

Date……..