The Holbeck Charitable Trust (a Company Limited by Guarantee)
Data Protection Policy
2016 Edition

1. Policy Statement

1.1 Everyone has rights with regard to how their personal data is handled. During the course of our activities we will collect, store and process personal data about our trustees, grant applicants and others, and we recognise the need to treat such data in an appropriate and lawful manner.

1.2 The types of personal data that we may be required to handle include details of current, past and prospective trustees, individuals associated with organisations who apply for grants from us and others who we communicate with. The data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 ("the Act") and other regulations. The Act imposes restrictions on how we may use that data.

1.3 This Policy does not form part of any contract of employment and it may be amended at any time. Where appropriate, we will notify data subjects of such amendments by mail or email.

1.4 Any breach of this Policy by a data user will be taken seriously and may result in disciplinary action.

2. Status of the Policy

2.1 This Policy sets out the basis upon which we (the company limited by guarantee known as The Holbeck Charitable Trust) will process personal data, our rules on data protection, and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal data.

2.2 The Data Protection Officer is responsible for ensuring compliance with the Act and with this Policy. That post is held by Mr John Lane, who can be contacted by telephone on 01904 625790 or by email at john.lane@rollits.com. Any questions or concerns about the operation of this Policy should be referred in the first instance to the Data Protection Officer.

2.3 If you consider that this Policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Data Protection Officer.

3. Definition of Data Protection Terms

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this Policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion about that individual, their actions and/or behaviour (such as a project evaluation). It includes personal data contained within emails.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our

business and our registration number with the Information Commissioner's Office for the purposes of the Act is Z3195328.

3.5 **Data users** are those of our employees, workers and trustees whose work involves using personal data. Data users must protect the information they handle by following this Policy and our other security policies and procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user but who processes personal data on behalf of a data controller and on a data controller's instructions. Employees, workers and trustees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good data protection practice. These provide that personal data must be:

4.1 processed fairly and lawfully;

4.2 processed for limited purposes and in an appropriate way;

4.3 adequate, relevant and not excessive for the relevant purpose(s);

4.4 accurate;

4.5 not kept longer than necessary for the relevant purpose(s);

4.6 processed in line with data subjects' rights;

4.7 secure; and

4.8 not transferred to people or organisations situated in countries without adequate protection.

5. Fair and Lawful Processing

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is processed fairly and without adversely affecting the rights of data subjects.

5.2 Each data subject must be told who the data controller is (in this case The Holbeck Charitable Trust), who the data controller's representative is (in this case the Data Protection Officer), the purpose for which their personal data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred. This includes our trust administrators Rollits LLP, who

manage grant applications centrally on our behalf and disclose any personal information contained therein to our individual trustees as part of the application assessment process.

5.3 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

5.4 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6. Processing for Limited Purposes

6.1 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

6.2. We use the data we hold about trustees and individuals associated with grant applicants (including information submitted on application forms and in correspondence with us) for administrative purposes - such as to direct communications, manage grant applications, monitor grants made and, where applicable, arrange payment of grants As a result, personal data regarding individuals associated with grant applicants, and regarding trustees, may be made available to our trustees, our trust administrators (Rollits LLP), our insurers, external auditors, contractors and other third parties (including third parties providing us with professional advice). Information relating to grant applicants may also be publicised in our annual Trustees' report and in our other publications, and we may also publish aggregated non-identifying information from time to time. Data subjects must be asked before their personal data is disclosed to any other third party, unless it is only acting as our data processor or such disclosure is required by law.

7. Adequate, Relevant and Non-Excessive Processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. Timely Processing

Personal data should not be kept longer than is necessary for the purpose or purposes for which it was collected. This means that data should be destroyed or erased from our systems (including data held in hard copy which is in the possession of any trustee, and data held electronically on an individual trustee's own computer system and other electronic devices) when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Data Protection Officer.

10. Processing in line with Data Subjects' Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

10.1 request access to any data held about them by a data controller;

10.2 prevent the processing of their data for direct-marketing purposes;

10.3 ask to have inaccurate data amended; and

10.4 prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. Data Security

11.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage or distress from such a loss.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if the data processor agrees in writing to comply with those procedures and policies, or if the data processor agrees in writing to put in place adequate measures himself/herself/itself.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

11.3.1 'Confidentiality' means that only people who are authorised to use the data can access it;

11.3.2 'Integrity' means that personal data should be accurate and suitable for the purpose for which it is processed; and

11.3.3 'Availability' means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore, where possible, be stored on a designated central computer system instead of individual PC's, laptops or other electronic devices.

11.4 Security procedures include:

11.4.1 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (personal data is always considered confidential);

11.4.2 Methods of disposal. Paper documents should be shredded. CD-ROMs and DVD-ROMs should be physically destroyed, and the contents of any portable media such as USB flashdrives deleted, when they are no longer required; and

11.4.3 Equipment. Data users should ensure that their portable IT equipment (which includes laptops, smartphones, tablets and USB flashdrives) are password-protected and encrypted, that individual monitors and other devices do not show confidential information to passers-by, and that they lock or log off from their computer or other device when it is left unattended.

12. Transferring Personal Data to a Country Outside the EEA

We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

12.1 the country to which the personal data is transferred ensures an adequate level of protection for the data subject's rights and freedoms;

12.2 the data subject has given consent;

12.3 the transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject;

12.4 the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or

12.5 the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subject's privacy, their fundamental rights and freedoms, and the exercise of their rights.

13. Disclosure of Personal Data

13.1 In addition to the potential disclosures referred to in paragraph 6.2 above, we may disclose personal data to third parties if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements, or where we are requested to do so by the Charity Commission, or to protect our rights, property or the safety of our employees, workers, trustees or others.

13.2 We may also disclose personal data to third parties in the event that we sell or buy any assets (in which case we may disclose personal data to the prospective buyer or seller of such assets), or if we or substantially all of our assets are acquired by, merged with or amalgamated with a third party, in which case personal data will be one of the transferred assets.

14. Dealing with Subject Access Requests

Data subjects must make a formal written request for information we hold about them. A fee is payable by the data subject for provision of this information. Any employee, worker, trustee or other individual/organisation acting on our behalf who receives a written request should forward it to the Data Protection Officer immediately.

15. Providing Information over the Telephone

Any employee, worker, trustee or other individual/organisation acting on our behalf dealing with telephone enquiries should be careful about disclosing any personal data held by us. In particular they should:

15.1 check the caller's identity to make sure that information is only given to a person who is entitled to it;

15.2 suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked; and

15.3 refer to the Data Protection Officer for assistance in difficult situations. No-one should be bullied into disclosing personal data.

16. Monitoring and Review of the Policy

16.1 This Policy is reviewed from time to time by the Data Protection Officer in consultation with our solicitors.

16.2 We will continue to review the effectiveness of this Policy to ensure it is achieving its stated objectives.