The Holbeck Charitable Trust (a Company Limited by Guarantee)
Data Protection Policy
2018 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 Personal 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 Personal Data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in DP Legislation. DP Legislation imposes restrictions on how we may use that Personal 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 this 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 Compliance Officer is responsible for ensuring compliance with DP Legislation 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 Compliance Officer.

2.3 If you consider that this Policy has not been followed in respect of Personal Data about yourself or other you should raise this with the Data Compliance Officer.

3. Definition of Data Protection Terms

3.1 **Controller** means the person or organisation that determines when, why and how to process Personal Data. The Controller is responsible for establishing practices and policies in line with the DP Legislation. We are the Controller of all Personal Data relating to our business and our registration number with the Information Commissioner's Office is Z3195328.

3.2 **Data Subject** means a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

3.3 **Data Users** are those of our employees, workers and trustees whose work involves using Personal Data. Data Users must protect the Personal Data they handle following this Policy and our other security policies and procedures at all times.

3.4 **DP Legislation** means the General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018 and all other data protection legislation having effect in the United Kingdom.

3.5 **Personal Data** means any information identifying an individual or information relating to an individual that can be identified (directly or indirectly) from that data alone or in combination with other identifiers in our possession or which we can reasonably access. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that individual's actions or behaviour.

3.6 **Processors** include any person or organisation that is not a Data User but who Processes Personal Data on behalf of a Controller and on a Controller's instructions. Employees, workers and trustees of Controllers are excluded from this definition but it could include suppliers which handle Personal Data on our behalf.

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

3.8 **Special Categories of Personal Data** means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. Special Categories of Personal Data can only be Processed under strict conditions, and will usually require the express consent of the Data Subject concerned.

4. Data Protection Principles

4.1 The main principles of DP Legislation are that Personal Data must be:

- Processed fairly and lawfully and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;
- accurate and up-to-date;
- kept only for as long as it is needed for the purpose for which it was collected; and
- Processed in a way that ensures appropriate security of the Personal Data.

We are required to demonstrate compliance with the above principles. In addition, Personal Data must be:

- Processed in accordance with the rights of the Data Subject to whom the Personal Data relates; and
- not transferred outside the European Economic Area unless adequate safeguards have been put in place to allow its export.

5. Fair, Lawful and Transparent Processing

5.1 The intention of DP Legislation is not to prevent the Processing of Personal Data, but to ensure that it is Processed fairly and without adversely affecting the rights of the Data Subject to which the Personal Data relates.

5.2 The Data Subject must be informed about, among other things, the identity of the Controller (in this case the Holbeck Charitable Trust), who the Controller's representative is (in this case, the Data Compliance Officer), the purpose for which the Personal Data is to be Processed by us, and the identities of anyone to whom the Personal Data may be disclosed or transferred. This includes our trust administrators Rollits LLP and the University of York, who manage grant applications centrally on our behalf and disclose any Personal Data contained therein to our individual trustees as part of the application assessment process.

5.3 Such information must be provided through an appropriate privacy notice or fair processing notice at the point of collection which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that the Data Subject can understand it. 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 In order for Personal Data to be Processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the Data Subject has consented to the Processing, or that the Processing is necessary to comply with a legal or contractual obligation, or for the legitimate interest of the Controller or the party to whom the Personal Data is disclosed. The Processing of Special Categories of Personal Data is prohibited unless certain additional conditions are met. In most cases the Data Subject's explicit consent to the Processing of such Personal 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 Personal Data was first collected or for any other purposes specifically permitted by DP Legislation. 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 Personal 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 applications (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 applications and regarding trustees, may be made available to our trustees, our trust administrators (Rollits LLP or the University of York), 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 out annual trustee's 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 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 Personal 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. Personal Data which is incorrect or misleading is not accurate and steps should 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 Personal Data should be destroyed.

9. Timely Processing

Personal Data should not be kept longer than is necessary for the purpose it was collected. This means that Personal Data should be destroyed or erased from our systems (including Personal 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 Personal Data is likely to be kept before being destroyed or reviewed, please contact the Data Compliance Officer.

10. Data Security

10.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised Processing of Personal Data, and against the accidental loss, destruction 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.

10.2 DP Legislation 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 Processor agrees to comply with those procedures and policies, or puts in place adequate measures himself/herself/itself.

10.3 Maintaining information security means guaranteeing the confidentiality, integrity and availability of Personal Data, as follows:

10.3.1 "Confidentiality" means that only people who are authorised to use the information can access it. **Personal Data is always considered confidential**;

10.3.2 "Integrity" means that Personal Data should be accurate and suitable for the purpose for which it is Processed; and

10.3.3 "Availability" means that authorised users should only 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 PCs, laptops or other electronic devices.

10.4 Security procedures include (but are not limited to):

10.4.1 Secure lockable desks and cupboards - desks and cupboards should be kept locked if they hold confidential information of any kind.

10.4.2 Methods of disposal - paper documents containing confidential information should be shredded. CD-ROMs and DVD-ROMs should be physically destroyed and the contents of any portable media such as USB flash drives should be deleted when they are no longer required.

10.4.3 Equipment - Data Users must ensure that their portable IT equipment (which includes laptops, smartphones, tablets and USB flash drives) 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.

10.4.4 Encryption - all portable devices must be encrypted before use to protect confidential information in the event of unauthorised access.

10.4.5 Data minimisation - we periodically review the Personal Data we hold. Any Personal Data which we no longer need, or which is held outside our retention periods will be disposed of.

10.4.6 Anonymisation / pseudonymisation - where appropriate, Personal Data should be anonymised or pseudonymised.

11. Processing in line with Data Subjects' Rights

Personal Data must be Processed in line with Data Subjects' rights. Data Subjects must be provided with information regarding the Processing of their Personal Data and (subject to limited exemptions) have a right to:

11.1 request access to any Personal Data held about them by a Controller; and

11.2 rectification of inaccurate Personal Data.

In certain circumstances, Data Subjects may also have the right:

11.3 to erasure of Personal Data;

11.4 of data portability (i.e. to request the transfer of Personal Data to another party);

11.5 to object to the Processing of Personal Data concerning him or her (including to prevent the Processing of their Personal Data for direct marketing purposes);

11.6 not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her;

11.7 to restrict the Processing of Personal Data (for example to ask to suspend the Processing of Personal Data to establish its accuracy or the reasons for processing it).

12. Transferring Personal Data to a Country Outside the EEA

We may only transfer Personal Data we hold to a country outside the European Economic Area ("EEA") if one of the following conditions applies:

12.1 The country to which the Personal Data is transferred is subject to an adequacy decision from the European Commission;

12.2 Appropriate safeguards have been implemented in respect of the transfer, for example:

a) the transfer is subject to use of a contract approved by the European Commission which gives Personal Data the same protection it has in the EEA; or

b) the transfer is to a third party based in the US which is part of the Privacy Shield which requires them to provide similar protection to Personal Data shared between the EEA and the US.

12.3 In the absence of an adequacy decision, or appropriate safeguards, one of the following applies:

a) the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards; or

b) the transfer is necessary for one of the reasons set out in DP Legislation, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject; or

c) the transfer is necessary for important reasons of public interest or necessary for the establishment, exercise or defence of legal claims.

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 is we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with a 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 Requests

Data Subjects may make a written request in respect of the Personal Data we hold about them in accordance with their rights which are detailed in paragraph 11. Such requests must be dealt with within a month from the receipt of the request and any Data User or other individual/organisation acting on our behalf who receives a written request should forward it to the Data Compliance Officer immediately.

15. Providing Information over the Telephone

Any Data User 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 Compliance Officer for assistance in difficult situations. No-one should be bullied into disclosing Personal Data.

16. Retention of Personal Data

We will only retain Personal data for as long as we need it for the purpose for which is was collected. Whilst taking in to consideration our legal obligations, we will on an ongoing basis: review the length of time we retain Personal Data; consider the purpose or purposes for which we hold the Personal Data for in deciding whether (and for how long) to retain it; securely delete Personal Data that is no longer needed for such

purpose or purposes; and update, archive or securely delete Personal Data if it goes out of date. For further information on how long we retain certain information please contact the Data Compliance Officer.

17. Reporting Breaches of Data Protection Legislation

If any Data User becomes aware that:

17.1 a device has been lost or stolen, or if a device may have been accessed by an unauthorised person or otherwise compromised;

17.2 there has been unauthorised access to any element of any equipment (including laptops, smartphones, tablets and USB flash drives), computer systems, premises or any other location where Personal Data is stored;

17.3 any Personal Data has been disclosed or accessed in error;

17.4 there is an IT threat; or

17.5 Personal Data has been compromised in any other way,

they must report the incident to the Data Compliance Officer immediately. In some circumstances we may be required to report the breach to the Information Commissioner's Office and the individual(s) concerned.

18. Monitoring and Review of the Policy

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

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