The Cellar Trust
Data Protection Impact Assessment (DPIA)

You should start to fill out this form at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting Controller Details	
Name of controller	The Cellar Trust
Subject/title of DPO	HR & Projects Manager
Name of DPO	Polly Mellor

Step 1: Identify the need for a DPIA
Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Migration to new online HR management provider (Breathe HR). This is because we are changing our external HR support and the existing online system is part of that old package. We have sourced a new online HR management system that we believe will be better and more efficient. We will be migrating personal data to this new system.

Step 2: Describe the Processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Data will be migrated from what we already hold on our existing system. It will also be added manually from paper records which will then be destroyed. Going forward we will collect the data from the data subjects themselves and potentially from some other sources such as referees, training providers, line managers and other colleagues. The data is used for the purposes of administering our employment contracts and volunteer agreements and managing the employment and volunteer relationship during the course of the person's work with us. We also process this data as there is a legitimate interest for The Cellar Trust to do so – namely to establish, exercise or defend legal claims. The data is stored on a cloud based platform. To achieve end-to-end security and end-to-end privacy all services are built in accordance with security best practices, privacy by design requirements and appropriate security controls. Breathe HR operates and maintains an Information Security Management System (ISMS) to control its information assets appropriately. Certification to the information security standard ISO 27001 was achieved in August 2018. The personal information held on Breathe HR may be shared internally with other authorised employees, e.g. managerial staff and HR staff but only for reasons relating to the employment or volunteering of that individual. We will only disclose information to third parties if we are legally obliged to do so or where we need to comply with our contractual duties. For instance we may need to pass on certain information to our external payroll provider or pension scheme, our HR management provider and professional advisers where necessary, who may be party to confidential discussions related to an individual. We require third parties to respect the security of the data and treat it in accordance with the law. We will share information with third parties where required by law, where it is necessary to administer our relationship with the individual or where we have another legitimate interest. We will only pass on an individual's information without their consent when there a situation that indicates they may be a danger to themselves or someone else, or information about a child at risk of harm or neglect. Data will not be transferred to countries outside the European Economic Area. Risks relate to the access of personal data by unauthorised persons. This is not deemed to be high risk.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Employee and volunteer data (contact details, emergency contact details, NI number, payroll number, details of supervision sessions, training records, job application and references, details of disciplinary and capability issues, sickness and other absence records, medical certificates and reports, risk assessments including criminal record risk assessments). Data will be collected and used frequently. Approximately 100 individuals are affected but this number will fluctuate. The geographical area is mainly West Yorkshire but is not limited to this area. For details of retention periods see our Data Protection Policy.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Relationship is as the employer or someone who engages volunteers. Employees will be able to add and amend contact details. All those affected will expect us to use their data in this way. Some volunteers may be vulnerable adults. The known concerns would relate to someone gaining unauthorized access or gaining access to then cause a data breach.

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
We do not feel it is necessary to consult regarding this change. This is because we are moving to a similar system with the same high level of security and data protection controls. We will continue to operate strict data protection measures in house. We have consulted Breathe HR before deciding to use their system to ensure they meet all the required levels of security and data protection and comply with GDPR. We are satisfied with this. We have also spoken with our existing provider regarding the data they will hold for us after the contract ends and they have explained they will hold this securely for a period of 6 years to comply with any requirement for legal claims.

Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The lawful basis is to comply with our contractual requirements and for the legitimate interest of establishing, exercising or defending legal claims. The processing achieves this purpose and is the most effective and secure way of doing so. We will ensure data quality by asking employees to keep their personal details up to date. We will undertake regular audits of the other data to ensure that it is being added correctly. We will delete data in accordance with our data retention policy to ensure data minimization. All individuals are given a Privacy Notice which explains how we process their personal data. They are also given access to our Privacy Policy, Confidentiality Policy and Data protection Policy. No data is transferred outside of the European Economic Area.

Step 5: Identify & Assess Risk

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Data breach – accidental	Possible	Severe	Medium
Data breach – intentional	Remote	Severe	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Data breach – accidental	Staff training	Reduced	Low	Yes
	Use of controls such as PC timeout, passwords not being retained etc	Reduced	Low	Yes
Data breach – intentional	Staff training eg whistleblowing, code of conduct	Reduced	Low	Yes
	Restriction of access	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Polly Mellor – DPO/HR & Projects Manager 04/02/2019	Already being actioned
Residual risks approved by:	Kim Shutler-Jones, CEO	No high risk
DPO advice provided:	04/02/2019	Ok to proceed as risk is low
Summary of DPO advice: OK to proceed as only low risk and suitable measures are in place.		
DPO advice accepted or overruled by:	Kim Shutler-Jones, CEO	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Polly Mellor - DPO	The DPO should also review ongoing compliance with DPIA