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 client management provider (MYMUP). We have sourced a new online client management system – MYMUP2, that we believe will be better and more efficient. We will be migrating personal data regarding our clients to this new system. This will apply to our Pathways to Employment and Haven clients only at this point.

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. Going forward we will collect the data from the data subjects themselves (clients) when referrals are made.

The data is used for the purposes of delivering our services, keeping records in line with our contractual requirements, providing clients with details of other services (with consent) and for monitoring and evaluation purposes (anonymised data only).

The data is stored on a cloud-based platform and is handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage. Data is protected via a secure server, dedicated IP & firewall. Threat monitoring software, anti-virus, anti-malware, IP Lockdowns, Log files, SSL Encryption, encrypted URLS and a pseudo-anonymization database structure are in place. MYMUP2 is annually Pen Tested and certified using the latest stack software and libraries

MYMUP complies with the NHS Standard Contract General Condition 21 linked to Patient Confidentiality, Data Protection, Freedom of Information and Transparency. MYMUP ensures that each system that it implements complies with the DCB0129 standard.

The personal information held on MYMUP2 may be shared internally with other authorised employees, e.g. managerial staff and other staff who may need to provide a service to that client; however, this is always on a need to know basis and with the principle of data minimisation in mind. This is standard practice and is explained within the Client Privacy Notice.

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.

Client data may also be shared with external services and professionals such as the Community Mental Health Team, job centre workers, GPs or care coordinators. This will only be done with the client's explicit consent and we will ask them to sign a form to say they agree.

We may have to share client data with other third parties who provide services for us, for example in connection with supporting our electronic client management system and IT network and professional advisers where necessary, who may be party to confidential discussions related to an individual.

We require all third parties to respect the security of thsi data and treat it in accordance with the law. We will share client data with third parties where required by law, where it is necessary to administer our relationship with the client or where we have another legitimate interest.

All our third-party service providers are required to take appropriate security measures to protect personal information in line with our policies. We only permit them to process personal data for specified purposes and in accordance with our instructions.

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?
Client record data which may include - contact details, demographic information, health information (e.g. details of support and/or therapy sessions, medication, mental and sometimes physical health conditions), information about employment status, education and training history This includes special category data. It may include criminal offence data as part of risk assessment reports. Data will be migrated from our current system and approximately 500 client records will be migrated. We will continue to collect new client data as we get new clients and as we have further contacts with existing ones. Data will be used to deliver our services. For details of retention periods see our Data Protection Policy. Approximately 500 individuals are affected by the data migration at present. The geographical area is mainly West Yorkshire but is not limited to this area.

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)?
The nature of our relationship is as a service provider. Clients need to give consent for us to store and use their data; they can also request copies of all data helpd about them, withdraw tehir consent for us to use their personal information (for some purposes), they can ask us to change inaccurate data; they can ask us to delete their personal information where it is no longer necessary for us to use it, they have withdrawn consent, or where we have no lawful basis for keeping it; they can ask for us to transfer their data to another party or restrict its use All those affected will expect us to use their data in the way outlined as it is the same way we currently use it. All our clients are vulnerable adults; we also may have some clients who are aged 16 and 17. 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 MYMUP 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 7 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 we use is consent. We will not pass on any data without consent except in exceptional circumstances, the lawful basis of which is vital interests. Examples of these circumstances might include information that suggests clients might be a danger to themselves or someone else, or information about a child at risk of harm or neglect. The processing achieves this purpose and is the most effective and secure way of doing so. We will ensure data quality by asking clients to update us of any changes to contact details. 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 minimisation. All individuals are given a Privacy Notice which explains how we process their personal data. They can also access via our website or on request 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 ShutlerCEO	No high risk
DPO advice provided:	20/04/2019	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, 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