Introduction

The Cellar Trust is committed to adhering to the legal safeguards within data protection legislation including the Data Protection Act 2018, the UK General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications (EC Directive) 2003.

The Cellar Trust respects the privacy of individuals and recognises how important it is that personal information remains secure. This policy sets out how we ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation. This policy covers employed staff, trustees and volunteers.

The GDPR provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of staff and volunteers and includes an expression of opinion about the individual and any indication of the intentions of staff and volunteers, or any other person in respect of the individual.

Sensitive personal data is defined as personal data relating to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Criminal proceedings or convictions

Depending on the reasons an individual interacts with us we may keep some or all of the following data about them:

- Clients – contact details, risk information, case notes including health related data.
- Volunteer information - application forms including referees, DBS information.
- Trustees – contact details, background information.
- Information on job applicants for posts, including references.
- Employee information – contact details, bank account number, payroll information, DBS information, supervision notes, health related information.
- Demographic information (e.g. age, gender, ethnicity)
- Donors – contact details, financial information.

The definition of 'processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes paper based and electronic personal data.

Roles and Responsibilities

All managers, staff and volunteers within The Cellar Trust will take steps to ensure that sensitive and personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

Employee	• Contractual responsibility to ensure all personal data is kept secure and processed in line with this policy and all relevant data protection legislation. • Report any data protection breaches immediately to their line manager.
Line Manager	• Monitors the processing of personal data and ensures staff are aware of and are adhering to the correct data protection and information governance (IG) procedures and protocols. • Reports any data protection breaches immediately to senior staff and / or the Information Governance (IG) Lead • Carry out regular Data Compliance Monitoring with support from the IG Lead
Chief Executive Officer (CEO)	• Appoints an IG Lead to help implement compliance with any legal requirements. • Delegates aspects of responsibility to relevant staff according to their organisational roles. • Instigates and oversees the investigation of confidentiality breaches and reports to the necessary bodies. • Reports any breaches or subject access requests to the board at appropriate intervals.
IG Lead	• Accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG.
Caldicott Guardian	• Responsible for promoting clinical governance or equivalent functions.
Senior Information Risk Officer	• Member of the trustee board who is responsible for managing information risks and to providing leadership and guidance from a senior level.

In addition to the above, The Cellar Trust is a Data Controller under the GDPR and we have responsibilities to ensure that our organisational and technical processes comply with the legislation. However, it is also the responsibility of all employed staff, trustees and volunteers who process personal information to ensure they not only understand but also act in line with this policy and the data protection principles.

Staff are responsible for ensuring that:

- They adhere to set procedures to ensure all personal data is kept securely.
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
- Personal data is kept in accordance with The Cellar Trust's data retention policy (see Appendix 1).
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the IG Lead if necessary.
- Any data protection breaches are swiftly brought to the attention of the IG Lead.
- Where there is uncertainty around a data protection matter advice is sought from the IG Lead.

Breach of this policy may result in disciplinary proceedings.

General Principles

Principles of Data Protection

In line with the GDPR principles, The Cellar Trust will ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified 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 reasons that data is processed.
- Accurate and kept up to date.
- Not held longer than necessary.
- Subject to appropriate security measures.

In addition to these principles we will adhere to the principle of accountability as set out in the GDPR legislation. We take responsibility for complying with data protection law at the highest management level and throughout our organisation. This includes keeping evidence of the steps we take to comply with the GDPR and ensuring we have appropriate technical and organisational measures and records in place which demonstrate our compliance.

Storage of Data

- All computer systems are password protected. Password protection is activated whenever a workstation is left unattended. Passwords are changed regularly (at least every three months). Staff are advised to follow guidance on using secure passwords, which can be found here: https://www.ncsc.gov.uk/
- All Cellar Trust mobile devices (laptops and tablets) are encrypted.
- Any mobile phone used for work purposes must either have finger print recognition or a pin code.
- Paper based personal data is kept to a minimum and steps are being taken to phase out paper based records. Any paper based data is kept in locked filing cabinets or locked desk drawers with restricted access.
- Staff are required to lock away any personal data whenever a work station is left unattended and adhere to our clear desk policy.
- Personal data is disposed of appropriately and securely e.g.: shredding, professional wiping of electronic records.
- Staff are not permitted to hold client data on memory sticks or portable devices. Staff using portable devices must only access The Cellar Trust documents and data via our secure, encrypted remote access Virtual Private Network (VPN) system.
- All of The Cellar Trust's electronic data is backed up remotely with a high degree of security by an authorised computer security business.
- IT hardware that contains data is disposed of in accordance with strict data protection processes. This is done by a third party who provide a certificate to show it has been wiped or disposed of correctly. Copies of these certificates are retained and available in request
- Cookies - we use cookies on our website. A cookie is a small file which asks permission to be placed on the website visitor's computer hard drive and it helps us to recognise and track users in order to provide them with a better online experience. Individuals can choose to accept or delete cookies. Please refer to our Privacy Policy for more information

Data Sharing

In the absence of consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to The Cellar Trust.

Third-Party Data Processors

Where external companies are used to process personal data on behalf of The Cellar Trust, responsibility for the security and appropriate use of that data remains with The Cellar Trust. Where a third-party data processor is used the following will apply:

- Any data processor chosen must provide sufficient guarantees about their security measures when protecting personal data.
- Reasonable steps must be taken to ensure that such security measures are in place.
- A written contract establishing what personal data will be processed and for what purpose must be set out.
- A data processing agreement must be signed by both parties and/or we will ensure that any external companies used have adequate processes in place which meet GDPR requirements.

For further guidance about the use of third-party data processors please contact the IG Lead.

Contractors, Short-Term Staff, Bank Workers and Volunteers

The Cellar Trust is responsible for the use made of personal data by anyone working on our behalf. Any contractors, short term or voluntary staff must be appropriately vetted for the data they will be processing. In addition The Cellar Trust will ensure that:

- Any personal data collected or processed in the course of work undertaken for The Cellar Trust is kept securely and confidentially.
- All personal data is returned to The Cellar Trust on completion of the work, including any copies that may have been made. Alternatively that the data is securely destroyed and The Cellar Trust receives notification in this regard from the contractor or short term / voluntary member of staff.
- The Cellar Trust receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor.
- Any personal data made available by The Cellar Trust, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from The Cellar Trust.
- All practical and reasonable steps are taken to ensure that contractors, short-term, bank or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the IG Lead.

Data Protection Compliance

In addition to the data protection and security measures already outlined in this policy, The Cellar Trust has in place a system of Data Protection Compliance Monitoring. We carry out regular spot checks to ensure that our staff are following the data protection guidance and procedures we have in place. The results of these checks are logged using a set format (spot check forms are available from the IG Lead and/or the server) and if we identify any issues from this process an action plan is recommended with a lead member of staff identified to ensure the actions are carried out.

Confidentiality

All Cellar Trust staff, volunteers and trustees are bound by the organisation's Confidentiality Policy and must adhere to certain ways of working to ensure we maintain strict confidentiality of personal data. Please refer to The Cellar Trust Confidentiality Policy for full details.

Data Subjects Rights

Data subjects are all those people we hold personal information about. Data subjects have rights in relation to the way we handle their personal data which include:

1. Where the legal basis of our processing is consent, to withdraw that consent at any time.
2. To ask for access to the personal data that we hold (see below).
3. To prevent our use of the personal data for direct marketing purposes.
4. To object to our processing of personal data in limited circumstances.
5. To ask us to erase personal data without delay:

    a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
    b. if the only legal basis of processing is consent and that consent has been withdrawn and there is no other legal basis on which we can process that personal data;
    c. if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;
    d. if the data subject has objected to our processing for direct marketing purposes;
    e. if the processing is unlawful.

6. To ask us to rectify inaccurate data or to complete incomplete data.
7. To restrict processing in specific circumstances e.g. where there is a complaint about accuracy.
8. To ask us for a copy of the safeguards under which personal data is transferred outside of the EU.
9. The right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with The Cellar Trust; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards.
10. To prevent processing that is likely to cause damage or distress to the data subject or anyone else.
11. To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
12. To make a complaint to the Information Commissioner's Office (ICO)
13. In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

Staff should ensure that all clients are given information about how we process their personal data, including information about their rights, when they first come into contact with The Cellar Trust. This is usually provided on the client consent form but staff should be aware that they can direct clients to the website for full details of our Client Privacy Notice and Privacy Policy and/or provide printed copies of our Client Privacy Notice and Privacy Policy on request. These documents can be found on the General Server in Staff Policies and Procedures.

Data Subject Access Requests

- Individuals have a right to access the personal data we hold about them. An individual can make a subject access request (SAR) to a member of staff verbally or in writing.

- It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point. This includes requests from staff and volunteers.
- A request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for their own personal data.
- If any member of staff is made aware of a request to access personal data they must report it to their line manager immediately who will deal with the request following the correct process. This will include reporting the request to the IG Lead.
- Requests must be complied with, usually within one month of receipt.
- A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.
- The person requesting the information should be asked to complete the Subject Access Request Form where possible although this is not compulsory. Whether or not a form is completed the Subject Access Log must be completed.
- ID - If there are doubts about the identity of the person making the request we will ask for more information. However, it is important that we only request information that is necessary to confirm who they are. We will let the individual know as soon as possible that we need more information from them to confirm their identity before responding to their request.
- The period for responding to the request begins when we receive the additional information.
- When sending the data to the individual who has requested it we must also provide a copy of the relevant Privacy Notice which covers information about what, how and why we hold their data.

Data Subject Access Requests – third parties

- We can respond to requests for personal data from a third party as long as we are satisfied that the third party making the request is entitled to act on behalf of the individual.
- It is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.
- If there is no evidence that a third party is authorised to act on behalf of an individual, we are not required to respond to the SAR.
- However, if we are able to contact the individual, we will respond to them directly to confirm whether they wish to make a SAR and then follow the process above.
- If we are satisfied that the third party has the appropriate authority, we will respond directly to that third party.
- If we think an individual may not understand what information would be disclosed, and in particular we are concerned about disclosing excessive information, we will contact the individual first to make them aware of our concerns.
- If the individual agrees, we may send the response directly to them rather than to the third party. The individual can then choose to share the information with the third party after reviewing it.
- If we cannot contact the individual we will provide the requested information to the third party (as long as you are satisfied that they are authorised to act on the individual's behalf).

Confidentiality Breaches

Any breach of any data protection, data security or confidentiality principles or procedures must be reported to the IG Lead who will launch an investigation process. Unlawful and / or inappropriate disclosure of personal information is a serious offence and will result in the Disciplinary Policy being invoked. Depending on the seriousness of the breach The Cellar Trust may also need to contact the local NHS Data Controller and ICO for advice and action. Any staff member who becomes aware of any confidentiality breach must inform their line manager or the IG Lead immediately. Failure to do so may result in disciplinary action.

New projects or systems - minimising data protection risks

Before any new project, plan or system is implemented or before changing anything already in place that involves processing personal data, The Cellar Trust will decide if a risk assessment should be carried out. If necessary, a Data Protection Impact Assessment (DPIA) will be conducted following the ICO guidelines. of any new project or plan that involves processing personal data.

Appendix 1: Data Retention Periods

1.1 Employee Records

Type of Record	Description of Record	Retention Period
Employee records (including bank workers)	Application forms and interview notes (unsuccessful applicants)	12 months after application date closes
	Application Form	Duration of employment
	Proof of Right to Work in UK	3 years after employment ends
	Personnel files and training records (including supervision, formal disciplinary records)	6 years after employment ends
	Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place
	Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years after employment ends, from the last financial year end
	Termination of employment, for example early retirement, severance or death in service	6 years after employment ends
	Pension records	Until the employee reaches age 84
	Statutory Sick Pay records, calculations, certificates, self-certificates	6 years after employment ends, from the last financial year end
	Working time records	2 years from date on which they were made
	Summary of record of service e.g. name, position held, date of employment	10 years after employment ends
	Payroll wage/salary records (also overtime, bonuses, expenses)	6 years from the end of the tax year to which they relate
	Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	6 years after the end of the tax year in which the maternity period ends
	Parental leave	18 years from the birth of the child
	DBS certificate information – certificate number and expiry date	6 years after employment ends
	DBS certificate information – (details of any cautions, convictions spent or otherwise that may be listed on a certificate)	6 months after a recruitment (or other relevant) decision has been made, unless exceptional circumstances

1.2 Volunteer Records

Type of Record	Description of Record	Retention Period
Volunteer records	Application forms and interview notes (unsuccessful applicants)	12 months after application date closes
	Application Form	Duration of volunteering
	Volunteer file and training records (including supervision, formal disciplinary records)	6 years after volunteering ends
	Expenses records	6 years from the end of the tax year to which they relate
	DBS certificate information – certificate number and expiry date	6 years after volunteering ends
	DBS certificate information – (details of any cautions, convictions spent or otherwise that may be listed on a certificate)	6 months after a recruitment (or other relevant) decision has been made, unless exceptional circumstances

1.3 Client Records

Type of Record	Description of Record	Retention Period
Client records	Clients who are referred but never seen (referral form and contact details)	1 year from the date of referral being received
Client records	Clients who receive a service - contact details, session notes, referral form. These records may include sensitive health related data and / or information about employment, education and training history	Client records are archived after 3 years from the date of the last entry (or for clients under 18 then until that person reaches the age of 21). Archive records are then accessible for a further 7 years after the date of archive. They are then permanently deleted.

1.4 Financial Records

NB. some financial data retention periods are listed under employee records

Type of Record	Description of Record	Retention Period
Accounting records	Bank statements, income and expenditure records, salary / payroll records	6 years from the last financial year end
Accounting records	Signed Annual Accounts and Reports	Permanently
Tax records	Income tax and NI returns, income tax records and correspondence with HMRC	6 years after the end of the financial year to which they relate.
National minimum wage records	National minimum wage records	6 years after the end of the pay reference period following the one that the records cover.

1.5 Health & Safety Records

Type of Record	Description of Record	Retention Period
Health and Safety	Accident books, accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).
Health and Safety	Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently