The Cellar Trust
Confidentiality Policy

Introduction

All Cellar Trust employees and volunteers are required to respect the right of clients, and of other employees and volunteers, to privacy and confidentiality as far as possible within the constraints of legal requirements and the safety of both the individual concerned and other people. A Confidentiality Policy is necessary for the following reasons:

- To protect clients, employees and volunteers from the possibility of information about them being passed on to individuals or organisations who have no right to that information.
- To reassure clients that good care will be taken with information they give to the Cellar Trust employees and volunteers and to be clear as to the circumstances when information can be shared with others.
- To provide guidance to employees and volunteers on the extent to which confidentiality is to be preserved, circumstances in which they may breach confidentiality, and measures to be taken for the safeguarding of information, in line with our obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).
- To assist The Cellar Trust employees and volunteers in complying with legal and statutory requirements for the disclosure of information.

All personal information held at The Cellar Trust will be treated as confidential. Mutual trust between The Cellar Trust and those using our services, or involved in their care, is central to the successful provision of services both to the individual client and to clients in general. All staff and volunteers have a duty to respect the confidentiality of clients or others who give information to the organisation.

Related Polices

- Code of Conduct
- Data Protection Policy
- Disciplinary Policy
- Equal Opportunities and Diversity Policy
- Grievance Policy
- IT Policy
- Privacy Policy
- Safeguarding – Vulnerable Adults
- Social Media Policy

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. This includes the following areas:

Employee Volunteer	• Contractual responsibility to safeguard all personal information and adhere to this policy in all areas of work. • Report any breaches of confidentiality immediately to their line manager.
Volunteer	• Responsibility to safeguard all personal information and adhere to this policy in all areas of work. • Report any breaches of confidentiality immediately to their lead contact or any other manager
Line Manager	• Monitor the processing of personal data and ensure staff are aware of and are adhering to the correct procedures and protocols. • Report any breaches of confidentiality immediately to senior staff and / or the Data Protection Officer (DPO). • Report subject data requests to the DPO.
Chief Executive Officer (CEO)	• Advise and support managers in the application of this policy and procedure. • Investigate confidentiality breaches and report to the necessary bodies. • Deal with subject data requests. • Report any breaches or subject access requests to the board at appropriate intervals.
Trustees	• Adhere to the principles of this policy. • Oversee the investigation of confidentiality breaches and ensure that the proper processes are followed. • Ultimate responsibility for ensuring compliance with the GDPR and any other relevant data protection legislation. • Ultimate responsibility for ensuring the correct policies and procedures are in place for recruiting and managing staff and volunteers

Personal Data

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.

For more details about what type of data we process and for what reasons please refer to The Cellar Trust's Privacy Policy and Data Protection Policy.

Consent

We will normally require consent when sharing personal information with anyone outside of the organisation, or where sharing takes place for purposes for which the information was not originally provided.

Consent must be 'informed'. This means that the person giving consent needs to understand why information needs to be shared, what will be shared, who will see their information, the purpose for which it will be used and the implications of sharing that information.

We will not share information with relatives, spouses, friends or advocates without the consent of the individual concerned. All enquiries for information, even if they are from close relatives, will be referred back to the client and the client's permission sought before disclosure if necessary.

In all circumstances where personal information is disclosed – whether with consent or under exception – no more information will be disclosed than is strictly required. We will follow strict process to protect the confidentiality of the personal information disclosed to the recipient agency and we will ensure that they have their own robust confidentiality and data protection procedures in place.

New and prospective clients will have our Confidentiality Policy explained to them and we will ask for their explicit consent to process their personal data when they are first in contact with the organisation. This consent will be recorded using the using the Client Agreement Form.

Data Sharing

Under specific circumstances related to safety, absolute confidentiality cannot be guaranteed and this will be made clear to clients at the point that they join the service, as part of the Client Agreement documentation. Under such circumstances, if it is thought necessary to pass on information to another individual or organisation this will be assessed on the basis of full consideration of whether there is a legal duty to disclose information.

An important part of our service provision includes working in partnership with other statutory and non-statutory organisations to achieve a joined up approach to care and support. In addition to this, as part of our Pathways to Employment service, clients may wish to undertake voluntary placements and qualifications or take part in work placements. This will involve liaising directly with other organisations. This will always be done in discussion with the individual client. These areas of data sharing are covered in the Client Agreement.

Please note that there is a separate Client Privacy Notice and a Data Protection Policy which cover data sharing and consent in more detail. In addition, there are specific data sharing agreements in place with our partner organisations.

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. The exceptions to this are as follows:

- The person needs urgent medical treatment.
- To protect children, young people and adults from harm.
- For the prevention or detection of a crime with the aim of protecting children, young people and adults from harm.
- In accordance with legal requirements (for example the Prevention of Terrorism Act, 2015) or order by the courts as part of legal proceedings. Where there is a legal requirement to breach confidentiality, the Chief Executive Officer must be informed.

Giving Information to the Police

There is no absolute duty to provide the police with information except in the case of suspected or actual terrorism. However The Cellar Trust's policy is that its employees and volunteers have a duty in the public interest not to withhold from the police any information concerning criminal activity of a serious nature. This should preferably be done with the knowledge of the person concerned and whenever possible with their co-operation but there may be circumstances where the risk to others is too great for this to be advisable or possible.

Requests from statutory bodies must be submitted in writing, even when there is a legal obligation on The Cellar Trust to comply with the request. Such requests must make clear on what basis the information is being requested and what the intended use of the information is.

There is a specific agreement relating to data protection and confidentiality practices for all third parties/contractors who deal with personal data (please refer to The Cellar Trust Data Protection Policy for more details).

Data Protection Processes

Client, staff and volunteer records and related personal data are stored and processed in line with our strict data protection principles, in line with the Uk General Data Protection Regulation (GDPR). Our electronic data is encrypted and stored on secure servers. We use a variety of security measures including passwords, encryption, firewalls and virus protection. See The Cellar Trust IT Policy for full details.

We are moving away from paper based records but any hard copy personal data is kept locked with restricted access.

Photography and other media

Being able to promote the work of The Cellar Trust is essential to the success of the organisation therefore we may ask individuals (clients, staff and volunteers) whether they would be willing to appear in photos, video footage or provide case studies which talk about the support they have received. Signed consent forms must be obtained before any photography, information or footage is used. Individuals will also have the opportunity to be featured anonymously, that is, their real name is not used. Individuals have the right to withdraw consent, in writing, after they have signed the form. However The Cellar Trust cannot guarantee that it will be able to withdraw any materials already used from circulation.

For more details regarding our data protection processes see The Cellar Trust Data Protection Policy.

Care of Information

The behaviours of our employees and volunteers are key to maintaining confidentiality within the organisation. They are required to adhere to the following confidentiality procedures (although this list should not be seen as exhaustive):

- Be mindful when discussing confidential information on the phone, or with clients or other staff / volunteers that they should not be overheard.
- To not disclose any client identifiable information in any public area including meetings and training sessions (with the exception of case meetings or one to one supervision).
- Keep the identity of any clients seen onsite confidential including if you know them in another capacity.
- Operate a clear desk policy and not to leave personal information in any area unprotected or unattended.
- Store all confidential electronic information on the organisation's secure client management and HR database systems (e.g. Lamplight, HR Online). If it is necessary to store personal data on the server this may need to be password protected or be in restricted folders.
- All personal data should be saved either on the server or cloud based database systems (as above) and not saved on desktops, laptops or memory sticks – hard copy data should be kept in locked draws and filing cabinets when not in use.

Any breach by staff of the above may result in disciplinary action. More details information and specific guidelines are available in the Cellar Trust Data Protection Policy and IT Policy.

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 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.
- 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 DPO.
- 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 Form where possible although this is not compulsory. Whether or not a form is completed the Subject Access Log must be completed.

- The identity of an individual requesting data under any of the rights listed must be verified and they will be asked to provide a recognised form of ID before any information is released.

For more details regarding the rights of data subjects see The Cellar Trust Data Protection Policy and Privacy Policy.

Confidentiality Breaches

Any breach of any data protection, data security or confidentiality principles or procedures must be reported to a senior manager or the DPO 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, Caldicott Guardian and Information Commissioners Office for advice and action.