Policy

Confidentiality/Data Protection

1 General Aims

1.1. The aim of the confidential Policy is to ensure a confidential service delivery and employment practice and to make sure people know their rights and responsibilities in accordance with The General Data Protection Regulation 2018 within the policy.

1.2. The Sanctuary Trust, as a data controller, takes the maintenance of confidentiality seriously. Any breach of this policy or its procedures which could lead to a disruption of relationships between staff, staff and service users, or the Sanctuary Trust and other agencies, or could lead to a breakdown of services may result in disciplinary action and will be reported the Information Commissioner's Office ICO. Contact admin@sanctuarytrust.org.uk to report any suspected breaches. Any person has the right to lodge a complaint directly with the ICO.

1.3. As a matter of good practice, other organisations and individuals working with the Sanctuary Trust, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that any staff who deal with external organisations will take responsibility for ensuring that such organisations sign a contract agreeing to abide by this policy.

2 Who is it for?

The policy is for the guidance and information of:

- Service users
- Staff
- Other stakeholders, agencies and individuals
- Management committee

3 General principles

3.1. Information will only be obtained and collected to ensure proper service delivery in its widest sense

3.2. Service users and staff have a right to know what information is held about them and why.

3.3. Personal information will be recorded in a way that is clear, honest, non discriminatory and objective.

3.4. Information may be in written form, on case notes, computer files, in letters to other agencies and individuals or may be verbal and not formally recorded. The policy applies whatever the form. A list of types of information is appended.

3.5. Care will be taken to ensure that all information is safely stored and secure, and only disclosed in accordance with these procedures.

3.6. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

3.7. All Sanctuary Trust computers have a log in system and our Contact Database is password protected, which allow only authorised staff to access personal data. Passwords on all computers are changed frequently. All personal and financial data is kept in a locked filing cabinet and can only be accessed by the Executive officers. When staff members are using the laptop computers out of the office care should always be taken to ensure that personal data on screen is not visible to strangers.

3.8. Data subjects are entitled to have personal data rectified if it is inaccurate or incomplete.

3.9. Data subjects can request the deletion or removal of personal data where there is no compelling reason for its continued processing.

3.10. We will allow data subjects, where appropriate, to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

3.11. Data subjects can object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

3.12. Anyone has a right to request information. The ICO information and guidance will be followed.

4 Information and Confidentiality

Project users

4.1. Information is collected about service users for the following reasons:

4.1.1. To ensure effective service delivery
4.1.2. To collect statistical information for management and government purposes
4.1.3. For other management purposes e.g. Housing Benefit.
4.1.4. To monitor equal opportunities and evaluate services

4.2. Only information required for effective service delivery will be recorded in a way that could identify any project user.

4.3. Information for statistical purposes or monitoring purposes will be "anonymous".

4.4. Information no longer required will be destroyed.

4.5. Service users have a right to see any information held about them providing this does not infringe another person's right to confidentiality.

4.6. Although staff members may be aware of a service users HIV status this will not be recorded even though this information may be relevant to service delivery (see HIV Policy). Symptoms and medication may be recorded if relevant to service delivery.

4.7. Recorded information is confidential to the service user, staff member(s) working with that individual and those who need to know to provide an effective service. Information that it is not necessary for other staff members to know for effective service delivery should remain confidential. Staff members unsure of whether there is a "need to know" should clarify this with the relevant line manager.

4.8. Information of a confidential or personal nature will not be shared with any outside agency without the informed consent of the service user. The Sanctuary trust reserves the right to withdraw this promise in cases of risk of danger or harm to the person, project or community, or in certain circumstances involving criminal practices. Where possible the service user will be informed of the disclosure.

4.9. Service users not satisfied that this policy and its procedures have been adhered to, or with the procedures themselves, should use the complaints procedure and have the right to lodge a complaint directly with the ICO.

4.10. All service users sign a disclaimer form to the effect that relevant/necessary information will be shared with other agencies

Staff

4.11. Information obtained about staff is normally related only to recruitment and employment. This will include some personal information such as date of birth, next of kin etc.

4.12. Information related to grievance, disciplinary, supervision, or training meetings, should be agreed with the other member of staff concerned.

4.13. No information about staff, whether formally or informally obtained should be disclosed without the consent of the staff member except as relates to management and supervision, normal employment activity, or service delivery. If it is necessary to provide any information to outside agencies or individuals, the informed consent of staff must be obtained, except in cases of risk of danger or harm to other members of staff, service users or others, or in certain circumstances involving criminal activity or gross misconduct.

4.14. Employment related information about staff may be shared with relevant parties, e.g. Housing Management. Staff will be informed in advance where possible. Personal information that is employment related, but which staff do not wish to be disclosed, should be discussed only with the project housing management and will only be disclosed if essential to good management of the project to the Chair.

4.15. Staff should have regard to the code of conduct expected of project employees in relation to safeguarding information about one another i.e. personal telephone numbers including information informally or accidentally obtained.

4.16. Staff not satisfied that this policy or its procedures have been adhered to, or with the procedures themselves, should use the complaints procedures.

4.17. For the purpose of funding or project development, information will be used anonymously or in cases where this is not appropriate service users will be made aware through consultation where they are able to opt out of information sharing.

Staff access to information

4.18. Staff will have access to all information pertaining to their areas of responsibility only.

4.19. All staff will make information available to relevant line managers. This will ensure continuation of services in the event of long term and/or permanent absence of any staff.

4.19.1. Extra keys will be held by line managers to allow access to lockable filing cabinets and drawers etc

4.19.2. Passwords to digital data and to access online services will be known to line managers

4.20. Extra sensitive digital data, such as recorded passwords, shall be encrypted using passwords of a minimum of seven digits and will include at least letters numbers and special characters to increase security against brute force recovery tactics.

Appendix of Types of Information Collected

Types of information that MIGHT be collected / recorded. This list is an example and is not exhaustive.

Service users

Financial	Contact with other agencies	Health
Personal details e.g. age	Behaviour / attitude in project	Religion / culture
Medical information	General correspondence	Family
Police record	Housing history	Education
Employment	History in project	Ethnicity
Information disclosed	Leaving inf. e.g. forwarding address	

Staff

Financial	Application forms	Supervision
notes Training reports/records	disciplinary records	Grievance
Record Sick/holiday leave	Personal e.g. Next of kin	Rota