

Policy

Confidentiality/Data Protection inc. GDPR

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. Sanctuary Trust, as a "data controller," is dedicated to safeguarding your privacy and protecting your personal data. This privacy notice serves to inform you of how we will handle and protect your personal data, as well as your privacy rights and the legal protections afforded to you. Please read this privacy notice in conjunction with any other privacy notice or fair processing notice we provide when collecting or processing your personal data, to fully understand how and why we use your data. We adhere to the General Data Protection Regulation (GDPR) 2018 when managing the personal information, you provide us and ensure that it is not misused. The GDPR defines a set of rules and guidelines, known as the General Data Protection principles, that we must follow when handling your information. Personal information shall be:
 - 1.2.1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
 - 1.2.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 - 1.2.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - 1.2.4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal information that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - 1.2.5. kept in a format which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed; personal information may be stored for longer periods insofar as the personal information will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
 - 1.2.6. processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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 at least 12 character and log on will be by 2 factor authentication. 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 include two factor authentication and meet NCSC data standards.

5 *GDPR Articles Referenced in this document.*

- 5.1. GDPR Article 15
https://sanctrust.sharepoint.com/:w:/g/EcLN-g_UE8VGmYAvYqc-VVUBFIB9wxgPi7babcTYkRwKgw?e=eSMPNM
- 5.2. GDPR Article 16
<https://sanctrust.sharepoint.com/:w:/g/EWm6RSHGLf9KoRydi6IHdA4BX-H79seSZqVt9xZUcbk8MQ?e=eiHpmR>
- 5.3. GDPR Article 17
<https://sanctrust.sharepoint.com/:w:/g/Ea0szqRbJGIDi9d4gHJa5jsBrXEYb-4Og23-VLrN9WwtYq?e=lthAG2>
- 5.4. GDPR Article 18
<https://sanctrust.sharepoint.com/:w:/g/EXFJli02isdMrL9NCPGChTEBEhB6eJX6ufjSWFov7VpHSw?e=sVmBaE>
- 5.5. GDPR Article 19
<https://sanctrust.sharepoint.com/:w:/g/ESgG2qXQdbFLkFgxJRYjN1YBE9Luy6bEN5ygAPmAO7e7uw?e=BEExbl>
- 5.6. GDPR Article 20
https://sanctrust.sharepoint.com/:w:/g/EblM-zW9UKtKnKMjBAzJ24QBR3Fo0GC6ZH4AIVlevJ2_IQ?e=jFSbbN
- 5.7. GDPR Article 21
https://sanctrust.sharepoint.com/:w:/g/EeqM5S8edStAj9G7N4_aqqUBJoUDljJgP9Naz_KBAfillMA?e=1iNfi9
- 5.8. GDPR Article 22
<https://sanctrust.sharepoint.com/:w:/g/EQVlpXgm8o9NhTZSPyy2qj4BilBealLwcHcVm7ndZOAxSA?e=KvD6pd>
- 5.9. GDPR Article 23
<https://sanctrust.sharepoint.com/:w:/g/EZ4mJYC4Mq5Plbp1d6w1MZUBS9C0E49djXlq33ao7-R1xw?e=FhLaQ6>

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

Wales Specific

Information specific for Welsh projects funded by the HSG.

Client specific information will be shared with our funders in line with our contractual agreements.

HSG operate their own confidentiality policy – this can be requested from supportingpeople@conwy.gov.uk

Your Rights -

- Under certain circumstances, you have rights under data protection laws in relation to your personal data. You can ask us to give you a copy of the personal data we hold about you and verify that we are processing it lawfully (known as a "data subject access request").
- You can ask us to correct any incomplete or inaccurate personal data we hold about you, though we may need to check the accuracy of any new data you provide.
- You can ask us to delete or remove your personal data if there is no good reason for us to continue processing it, or if you have successfully objected to its processing, or if we processed it unlawfully, or if we are required by law to erase it. However, we may not always be able to comply with your request for specific legal reasons that we will inform you of at the time of your request.
- You can object to the processing of your personal data if we are relying on our legitimate interests (or those of a third party) and there is something about your situation that makes you want to object as you feel it affects your fundamental rights and freedoms. You can also object if we are processing your personal data for direct marketing purposes. However, we may have compelling legitimate grounds to continue processing your data which override your rights and freedoms.
- You can ask us to suspend the processing of your personal data in certain situations, such as if you want us to verify the accuracy of the data, if our use of the data is unlawful but you don't want us to delete it, if you need us to keep the data even if we no longer require it as you need it to establish, exercise or defend legal claims, or if you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- You can withdraw your consent at any time if we are relying on your consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you, and we will let you know if this is the case.

You have the right to complain to the Information Commissioner's (ICO) Office if you think there is a problem with the way in which Sanctuary Trust are handling your information. To contact the ICO, please call 0303 123 1113 or visit their website at <https://ico.org.uk/>