City of Sanctuary

Data Protection Policy and Procedures

1. Introduction

This policy applies to City of Sanctuary (registered charity no. 1124921), including the Asylum Matters project.

Our definition of **'personal data'** is: information about a person which is identifiable as being about them. It can be stored electronically or on paper, and includes images and audio recordings as well as written information.

Our definition of **'senstive personal data is'** is: information pertaining to an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.

City of Sanctuary is the **'controller'** of personal data.

2. Responsibility

The named individual with responsibility for GDPR compliance is Sian Summers-Rees (CoS Chief Officer).

All staff will read this document and be familiar with the principles of the General Data Protection Regulation contained within it (see above). When carrying out project activities, all staff will consider the basis on which data is being stored or processed, and implement safeguards as appropriate.

The Data Protection Policy will stand as an agenda point at both City of Sanctuary and Asylum Matters project team meetings on an annual basis to ensure that staff are aware of this policy and relevant developments insofar as they relate to data protection. An annual review of compliance with policy will be carried out at this meeting. Actions for staff to carry out in respect of data retention and disposal will be carried out in advance of the meeting.

3. Data Protection Principles

We will work in compliance with the principles of the GDPR:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2 is met*, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

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

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

*The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary:
- in relation to a contract which the individual has entered into; or
- because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition.

4. Collecting and Processing Personal Data

The legal bases under which data can be processed are as follows:

a) Consent: the individual has given us clear consent for us to process their personal data for a specific purpose
b) Contract: the processing is necessary for a contract we have with an individual, or because they have asked us to take specific steps before entering into a contract.
c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
d) Vital interests: the processing is necessary to protect someone's life.
e) Public task: the processing is necessary for us to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

In addition, we may occasionally gather data from people who are or have been in the asylum system and this data may sometimes be of a sensitive nature and constitute special category data under Article 9 of the GDPR (information pertaining to an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation)

The applicable additional conditions (GDPR Article 9 conditions) for processing such data are conditions (a) and (d):

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

5. Consent:

When relying on consent to gather and hold the data of individuals, consent gained must be:

- **Unambiguous:** it must involve a clear affirmative action (eg an opt in, a signature, an email confirming consent has been given)
- **Granular:** it must be clear what consent is being given for
- **Recorded:** clear records should be kept of consents that have been given
- **Can be withdrawn:** individuals giving their consent for us to process their information must be made aware at the time that the consent can be withdrawn

In the vast majority of cases, it will be appropriate that consent forms are amended specifically for any data gathering exercise (eg gathering of evidence submissions). It will be appropriate to rely on consent when any data is being gathered for disclosure outside the organisation which could identify an individual who is or has been in the asylum system (see section 3 below).

Our requests to gain consent should include: the name of the project and organisation; the name of any third party controllers who will rely on the consent; why we want the data; what we will do with it; and the fact that individuals can withdraw consent at any time.

Where consent is relied upon and has not been obtained, information should not be stored or processed.

The issue of consent will be reviewed annually to ensure our procedures are up to date

Relevant documentation: Consent form / privacy notice; photo release form.

6. People who are or have been in the asylum system

Whenever staff are dealing with the personal data of people who are or have been in the asylum system (including photographs), consideration should be given to whether the data is special category data under the meaning of Article 9 of the GDPR:

- Does the information pertain to an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation?

In addition staff members should consider:

- Is there any information which could serve to identify the individual or sensitive information about them to a third party?

In the majority of cases the legal basis for processing this data will be consent and this should be explained, sought and recorded accordingly. Any case where it is considered that the basis for processing data is the legitimate interests of the organisation rather than consent, and information held is capable of identifying an individual should be referred to line management. If the data collected is of a sensitive nature, information which could identify an individual to a third party must not be disclosed outside the organisation and every effort must be made to ensure that data held within the organisation is made secure (ie data should be anonymised / pseudonyms should be used and specific information which could identify an individual to a third party should be edited out). Photographic data is considered separately (see section below).

Relevant documentation: consent form

7. Photographic data

There is a legitimate expectation that photographs taken at public events can be made public. However, no photograph which could identify an individual who is or has been in the asylum system should be published online without consent for this purpose first having been obtained.

Relevant documentation: photo release form

8. Right of access

Individuals have the right to obtain: confirmation that we are processing their data, access to the data we hold about them and other supplementary information (information in our **privacy notice**). They can request this information verbally or in writing.

On receipt of such a request we will provide information to them about what data we hold without delay and at most within one calendar month. We may extend this deadline by another two months for complex or numerous requests (in which case we must inform the individual and give an explanation). We must verify the identity of the person making the request using "reasonable means". If the request is made electronically, we will provide the information in a commonly used electronic format.

Relevant documentation: consent form / privacy notice

9. Right of rectification

Individuals have the right to have personal data rectified if it is inaccurate or completed if it is incomplete. An individual can make a request for rectification verbally or in writing.

On receipt of such a request we will rectify information held on that individual without delay and at most within one calendar month. We may extend this period by a further two months for complex or numerous requests. We must verify the identity of the person making the request using "reasonable means". If we have shared the incorrect information with other organisations, we will inform them of the rectification where possible.

10. Right of erasure

Individuals have the right to be forgotten and can request the erasure of personal data. An individual can make a request for erasure verbally or in writing.

On receipt of such a request we will erase information held on that individual without delay and at most within one calendar month. We may extend this period by a further two months for complex or numerous requests. We must verify the identity of the person making the request using "reasonable means".

There are limited circumstances in which such a request can be refused including: to exercise the right of freedom of expression and information, to comply with a legal obligation, or to exercise or defend legal claims. If any of these apply, further advice should be sought before information is erased.

11. Right to restrict processing

Individuals have the right to restrict processing of their data. They can request that processing be restricted verbally or in writing.

On receipt of such a request we will respond without delay and at most within one calendar month. We may extend this period by a further two months for complex or numerous requests. We must verify the identity of the person making the request using "reasonable means".

As a matter of good practice, we will consider restricting the processing of personal data if requested to do so. When processing is restricted, we are permitted to store the personal data, but not further process it, and may retain just enough information about the individual to ensure that the restriction is respected in the future. If we have disclosed personal data to other organisations, we must inform them about the restriction, unless it is impossible or involves disproportionate effort to do so.

12. Right to object

Individuals have a right to object to the processing of their personal data.

On receipt of an objection to the processing of an individual's personal data we will stop processing that data without delay unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims. On receipt of such a request we will respond without delay and at most within one calendar month.

We may extend this period by a further two months for complex or numerous requests. We must verify the identity of the person making the request using "reasonable means"

13. Procedures

We will collect the following kinds of personal data:

Newsletter mailing list (MailChimp)

Supporter email addresses will be collected via an online newsletter sign-up form or via events or other forms where their explicit consent is given via a tick box to sign up to the newsletter.

The lawful basis for processing this data is consent or legitimate interest.

Supporter email addresses for the newsletter mailing list are stored on MailChimp and newsletters are sent out only via MailChimp.

Each newsletter has the option for the individual to unsubscribe and they can also unsubscribe any time via the MailChimp website. Email addresses will be kept on the mailing list until requested to be removed by the individual or where there is a bounce and the email address is automatically removed.

Where consent is given via a paper form, the form will be stored in a locked filing cabinet. Every two years, paper records will be reviewed against MailChimp's records and anyone that has unsubscribed will be blacked-out from the paper record.

Website

User email addresses and IP addresses are stored on our website database.

The lawful basis for processing this data is consent. All users are set up through requesting access and then activating their account themselves.

Data will be stored on the website database until requested to be removed by the individual. Every two years, user activity will be reviewed and any users that have not been active for two years will be removed.

Advice will be taken to ensure the security of the website server.

Expense forms

Expense forms include individual names and bank details.

The lawful basis for processing this data is consent.

Expense forms will be kept for seven years to comply with HMRC requirements. All expense records are kept in a locked cabinet.

Beneficiary bank details are stored online via the Co-operative Bank online banking system. Any beneficiary record that has not been active for seven years will be deleted.

Event bookings

Necessary personal data will be provided by the individual via an online form and processed for the purpose of providing information about that event. There will be a separate tick box on the form to provide consent to be added to our mailing list.

The lawful basis for processing this data is consent.

Event booking data will be stored for three years after the event.

Trustee information

New trustees will be asked to complete an online form including necessary information. There will be a separate tick box on the form to provide consent to be added to our mailing list.

The lawful basis for processing this data is consent and to fulfil our legal obligation to provide this information to the Charity Commission and our bank, when requested.

Trustee information (name, address, phone number, email address) will be stored for seven years after the trustee steps down.

Employee personal information

New employees are required to complete a starter form which is provided to our payroll company in order to be able to pay them.

The lawful basis for processing this data is consent and to meet our contractual obligations.

Employee information will be stored for seven years after the employment contract has been terminated.

Group contacts

When a new group registers, they provide necessary personal data via an online form. They can choose which addresses are made public via the website and which are used only by CoS staff for the purpose of contacting them with useful information. There is a separate tick box on the form to provide consent to be added to our mailing list. There is no requirement for groups to use personal email addresses; a CoS email address can be provided on request.

The lawful basis for processing this data is consent or legitimate interest.

Group contacts can request to be removed from this list at any time by contacting info@cityofsanctuary.org

We will undertake a review of group contacts every two years by writing to all groups to ask them to confirm their details. Any details that are no longer valid or where there is no response will be deleted.

Partners / media contacts

Individuals on these lists will only be added if appropriate and contacted on the basis that we have a legitimate interest in contacting them that does not affect their rights.

Other mailing lists / contact lists

Some contact lists are stored in staff email accounts. Email addresses will be collected with explicit consent, where there is a legitimate interest to contact that person or where they are publically available.

The lawful basis for processing this data is consent or legitimate interest.

Contacts can request to be removed from this list at any time by contacting the relevant staff member. Email addresses will be kept on the mailing list until requested to be removed by the individual or where there is a bounce and the email address is automatically removed.

Membership list

New members provide necessary information via a form. There will be a separate tick box on the form to provide consent to be added to our mailing list.

The lawful basis for processing this data is consent and to meet our legal obligation to keep a list of members.

The membership list is renewed annually and lists from previous years will be kept for seven years afterwards.

Photos

There is a legitimate expectation that photographs taken at public events can be made public. However, no photograph which could identify an individual who is or has been in the asylum system should be published online without consent for this purpose first having been obtained.

Photo consent forms will be signed where it is intended to use the photo for publicity purposes and no photo will be used for publicity purposes without explicit consent for that purpose.

The lawful basis for processing this data is consent.

Sensitive personal data

Please see above section on **'People who are or have been in the asylum system'.**

Additional types of data

For any additional types of data held in the future, the lawful basis will be established by agreement between 2 or more members of the staff team and documented through an appendix to this policy.

14. Data Security

- It is our objective that all personal data will be stored on our own secure database. In the meantime, all personal data should be stored on Google Drive.
- All staff should have a secure password to access Google Drive and any computer where their Google Drive password is saved should be accessed via a secure password
- Password security can be checked via https://howsecureismypassword.net/ (secure passwords are longer and contain a mixture of letters, numbers and characters and do not contain words or names)

- Passwords shouldn't be written down so staff should have some way of remembering them (or use LastPass)
- Staff should limit the number of devices where their Google Drive password is saved and should be careful not to save their password on to any device that is accessible by others
- Any paper records containing personal data should be stored in a locked cabinet
- Where possible, any mail-out to bulk contacts should be sent via a distribution list or via MailChimp. Where this is not practical, care should be taken to ensure all contacts are listed under **bcc:**
- No personal data should be given out except with explicit permission for that specific purpose eg. if someone is interested in joining a group and that group has a contact email they are happy to be shared
- No personal data will be stored on unencrypted memory sticks
- All staff have a confidentiality agreement as part of their employment contract and any volunteers are required to sign a confidentiality agreement. Any staff or volunteers that leave will have their access to Google Drive removed.

15. Data sharing

The following principles will apply for data sharing:

- there is a good reason for the sharing to take place
- the individuals have been made aware their data is being shared.
- the minimum amount of personal data is shared.
- the sharing is for the minimum time and it is clear what then happens to the data.
- the sharing is done as securely as appropriate for the data involved.
- the sharing is documented.

A Data Sharing Agreement is in place with Places of Sanctuary Ireland (POSI) so that data may be shared for joint purposes:

- Access to Irish and Northern Irish group sites on our website
- Access to group contacts information with the purpose of keeping the Irish and Northern Irish group information up to date

Data provided as part of event bookings may also be shared with local CoS groups for the purpose of the organisation of the event only and on the understanding that it is deleted by that group after the event.

16. Mobile working guidelines (laptops and phones):

- Appropriate passwords should be set for any device used to access personal data
- A password protected screen lock / screen saver should be configured
- The device should be set to autolock after a period of no more than 10 minutes

- Operating systems should be kept up to date and appropriate anti virus software used
- Minimise the amount of personal data stored on mobile devices (eg laptop hard drives)
- Be mindful of the risks of using unsecured wireless networks
- Precautions should be taken to ensure that family / friends cannot access information
- Precautions should be taken to guard against theft

17. Data retention and disposal

It is good practice to ensure that no more personal data than is necessary for our legitimate purposes is retained. Staff should ensure that unnecessary personal data, for example in email accounts, is erased on an ongoing basis. On an annual basis, an exercise will be undertaken to ensure that personal data which is no longer necessary for our legitimate core activities is removed and a record shall be kept that this exercise has taken place and what data has been disposed of.

18. Data breaches

A data breach is the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All staff members have a duty to report accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data to the City of Sanctuary Chief Officer or Asylum Matters Project Director who will record the breach and determine whether the breach is notifiable to the Information Commissioner's Office. Any notifiable breaches will be reported to the Information Commissioner's Office within 72 hours.

Privacy Notice - Your Personal Data

What we need

City of Sanctuary will be what's known as the 'controller' of the personal data you provide to us. We only collect basic personal data about you which does not include any special types of information or location based information. This may however include name, phone number, email etc

City of Sanctuary

We may also take your photo if we have your consent to do so.

Why we need it
We need to know your basic personal data in order to provide you with information via our newsletter plus any important updates via email. We are legally required to keep a list of members. We will not collect any personal data from you that we do not need.

Photos will be used for publicity purposes.

What we do with it
All the personal data we process is processed by our staff in the UK and Ireland. However, for the purposes of IT hosting and maintenance, this information is located on servers both within and outside the European Union.

We have a Data Sharing Agreement in place with Places of Sanctuary Ireland (POSI), for the purpose of keeping group contact information up to date. Data provided as part of event bookings may be shared with local CoS groups for the purpose of organising that event. No other third parties have access to your personal data unless the law allows them to do so. We have a Data Protection regime in place to oversee the effective and secure processing of your personal data. Please contact us for more information about this framework.

How long we keep it
The list of members is kept for three years. The information we use for marketing purposes will be kept until you notify us that you no longer wish to receive this information or no longer wish for your data to be held. Please contact us for more information about our retention schedule.

What are your rights?
If at any point you believe the information we process on you is incorrect, you can request to see this information and have it corrected or deleted. If you wish to raise a complaint on how have handled your personal data, please contact us. If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law, you can complain to the Information Commissioner's Office (ICO).

Contact

City of Sanctuary
4th floor, Oak House
94 Park Lane
Leeds LS3 1EL
Tel: 0113 3862224
Email: info@cityofsanctuary.org

City of Sanctuary

asylum matters

Asylum Matters Privacy Notice

1. **Your personal data – what is it?**

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

2. Who are we?

Asylum Matters is a project hosted by City of Sanctuary (Registered Charity 1124921), which is the 'data controller' for the personal data collected by the project. This means it decides how your personal data is processed and for what purposes. City of Sanctuary can be contacted at City of Sanctuary, 4th Floor, Oak House, 94 Park Lane, Leeds LS3 1EL, and at info@cityofsanctuary.org. You can contact also Asylum Matters project staff directly at info@asylummatters.org.

3. What is the legal basis for our processing of your data?

The legal bases under which personal data is processed by the "Asylum Matters" project are as follows:

g) Consent: you have given us clear consent for us to process your personal data for a specific purpose;
h) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Our legitimate interests in the processing of personal data are the furtherance of our campaign goals in accordance with our project mandate and the charitable objectives of City of Sanctuary.

4. What data do we collect?

Our collection of personal data is limited to that data necessary to fulfil our project mandate. This is normally confined to contact details of supporters of our campaign goals and other correspondents and business contacts contacted in the course of our campaigning work.

We use the personal data of supporters of our campaign goals and other correspondents and business contacts contacted in the course of our campaigning work:

1) to contact them with relevant updates on developments in the sector or calls to action on our campaign goals;
2) to inform our campaigning work;

3) to contribute to the efficacy of our public campaigning work

We also gather data from people who are or have been in the asylum system to inform our campaigning and this data may sometimes be of a sensitive nature. In this case, additional conditions and safeguards for processing your information apply.

We comply with our obligations by not collecting or retaining excessive amounts of data; by keeping personal data up to date; by storing and destroying it securely; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data. We have a Data Protection policy to oversee the effective and secure processing of your personal data, and implement annual reviews of what data we hold and whether it is still necessary for us to hold it. Please contact us for more information about this framework.

All the personal data we process is processed by our staff in the UK. However, for the purposes of IT hosting and maintenance, this information may be located on servers outside the European Union. Please see here for details of our business services provider's compliance with GDPR, including appropriate certifications.

5. Sharing your personal data

Your personal data will be treated as strictly confidential. We will only share your data with third parties outside Asylum Matters / City of Sanctuary with your consent.

6. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data
- The right to request that we correct any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for us to retain such data;
- The right to withdraw your consent to processing at any time
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data
- The right to lodge a complaint with the Information Commissioner's Office.

If at any point you believe the information we process on you is incorrect, you can request to see this information and have it corrected or deleted. If you wish complain about how have handled your personal data, please contact us. If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law, you can complain to the Information Commissioner's Office (ICO).

8. Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

9. Contact Details

To exercise all relevant rights, queries or complaints please in the first instance contact info@cityofsanctuary.org or info@asylummatters.org