Data protection procedures

Date written: April 2023	Version: 3
Date due for review: April 2024	Amendments:

Purpose	Scope
This policy outlines the principles of data protection and the guidance to follow.	This policy and procedure applies to all current staff members and volunteers, whether full or part-time, temporary or fixed-term.

All employees are bound by a legal duty of confidence to protect personal identifiable and confidential information ('personal data') they may encounter during the course of their work. The following procedures must be adhered to.

General

Personal data must be effectively protected against improper disclosure when received, stored, transmitted or disposed of. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 requires personal data to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Employees must familiarise themselves with the Voices in Exile Data Protection Policy, the principles of the GDPR and, when carrying out their duties, consider the basis on which data is being collected, stored or processed and implement safeguards as appropriate.

It is strictly forbidden for employees or volunteers to knowingly browse, search for or look at any information controlled by Voices in Exile that relates to themselves, or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and may constitute a breach of the Data Protection Act 2018.

In addition:

- Access to personal data must be on a need-to-know basis.
- Disclosure must be limited to that purpose for which it is required.
- Personal data, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

Physical location

- Access to rooms and offices where personal data is stored must be controlled and doors locked at the end of each day. Measures should be in place to prevent oversight of personal data by unauthorised parties when sharing office space with others.
- At the end of each day, all employees and volunteers should make sure their desk tops are clear of any records containing personal data. In particular, they must keep all case files in recognised filing and storage places that are locked.
- Unwanted printouts containing personal data must be put into a confidential waste bin. Documents and other media containing personal data and other confidential information must not be left unattended, but filed and locked away when not in use.
- If employees or volunteers need to take personal data home or on outreach work, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family, friends or colleagues must not be able to see or have access to the information and appropriate safeguards must be in place against theft.

Information held on computer or other devices

- Employees must not store client's personal data on a privately owned computer or device.
- No personal data will be stored on unencrypted memory sticks.

- Appropriate passwords will be set for any device used to access personal data. A password protected screen lock / screen saver will be configured. Devices will be set to autolock after a short period e.g. 10 minutes.
- Operating systems will be kept up to date and appropriate anti-virus software used.
- The amount of personal data stored on mobile devices will be minimised commensurate with the purpose for which the device is used.

Working from home

- Access to laptops and devices will be password-protected or encrypted, including use of screen lock or timeout screen.
- Only approved technology will be used for handling personal data. Only approved hardware and the software provided will be used for home working. This will be via licensed Microsoft Office software and Microsoft Teams cloud storage.
- The organisation's data will not be mixed with personal data. If staff have to work using their own devices, work data must be kept separately to avoid accidentally keeping hold of data for longer than is necessary. Work documents will not be stored on desktops, particularly if other members of the household might access the device. Documents in download folders will be deleted regularly and at least weekly.
- Home working spaces may unavoidably be shared with other members of the household. Conversations should be held where they are less likely to be overheard and screens positioned where they are less likely to be overseen.
- Confidential data should not be printed if possible. If sensitive documents or hard copies of client data do need to be kept at home, they must be stored safely until they can be taken into the office and disposed of securely. Hard copies of work documents or confidential client data must not be left on surfaces where they can be seen by other household members. If a home shredder would help to more effectively manage this, this should be discussed with a manager.
- To avoid loss or theft of personal data, print outs and devices should be put away at the end of the working day if possible.
- Staff need to be extra vigilant about opening web links and attachments in emails or other messages. Unfamiliar web links or attachments claiming to give important coronavirus updates should not be clicked on. Follow the National Cyber Security Centre's (NCSC) guidance on spotting suspicious emails.
- Whether using online storage, a laptop or some other technology, it is important to make passwords hard to guess. The NCSC recommends using three random words together as a password (e.g. 'coffeetrainfish' or 'walltincake'). Different passwords should be used for different services.
- Staff will communicate securely and take extra precautions when sending documents by email. Outlook email, our WhatsApp staff or individual project chat groups, Microsoft Teams and telephone will be used. Home or personal email accounts should never be used to send work or sensitive client data. If data does need to be shared with others then a secure messaging app or online document sharing system will be used. If email has to be used, documents will be password protected and passwords shared via a different channel, like text.

- Keep software, operating systems and security software up to date to make it more difficult for hackers to get in.

Use of email

- Personal data may only be transmitted by email to an email address which is known to the relevant Voices in Exile employees.
- Employees must not forward any personal data via email to their home e-mail account.
- Personal data must not be sent by unencrypted attachment to email.
- Where possible, any mail-out to bulk contacts will be sent via a distribution list or via MailChimp. Where this is not practical, care will be taken to ensure all contacts are listed under bcc unless there is prior agreement from all recipients to the communication being open.

Use of passwords

- Individual passwords must be kept secure and must not be disclosed to others.
- Personal data files will be password protected.

Data retention

- Employees must familiarise themselves with the Voices in Exile Data Assessment, which is appended to this document.
- Employees will 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.

Subject access requests

Individuals for whom Voices in Exile hold personal data have the following rights: right of access, right to rectification, right of erasure, right to restrict processing and right to object. Employees who receive such a request should promptly acknowledge receipt and forward the request to the Director.

Reporting of breaches or risk of breaches

The Director is responsible for leading on the protection of confidentiality within Voices in Exile as well as ensuring that confidentiality requirements are reflected in our strategies, policies and procedures. Any risks and incidents regarding confidentiality should be reported to the Director.

Any employee who considers that data protection policies or procedures may have been breached (including by the disclosure of personal information) should raise the issue with the Director. The Director will determine if the breach is notifiable to the Information Commissioner's Office.

Privacy notices and form of authority

Members of staff will use the Privacy Notices at **Appendix 1** to inform relevant groups of people about how Voices in Exile deals with their personal information and their rights. Service users will be asked to give their consent to the handling of their personal data by completing the Form of Authority at **Appendix 2**.

Data assessment and associated provisions

Voices in Exile collects, stores and processes the following categories of data and will observe the associated provisions.

Trustee information

New trustees will be asked to complete a hard copy or 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

Employee data includes contact details, bank account details, payroll information, supervision and appraisal notes. 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.

Supporter information

Individual supporters of Voices in Exile provide necessary information via an online or hard copy form. There will be a separate tick box on the form to provide consent to be added to our mailing list. There will be a separate tick box whereby supporters may consent to their financial details being retained for future further donations.

The lawful basis for processing this data is consent or legitimate interest and to meet our legal obligation to keep a list of supporters and their financial contribution.

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. Details of supporters will be kept for seven years after their last contribution.

Volunteers

Volunteers are required to complete a starter form providing basic information. The lawful basis for processing this data is consent or legitimate interests. Volunteer information will be stored for seven years after the relationship has been terminated.

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 securely in a locked cabinet or electronically with access only by relevant staff. Beneficiary bank details are stored online via the Royal Bank of Scotland 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 or hard copy 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.

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 details are stored in employees' email accounts. Email addresses will be collected with explicit consent, where there is a legitimate interest to contact that person or where they are publicly 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 employees. 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.

Photos

There is a legitimate expectation that photographs taken at public events can be made public. However, no photograph which could identify a service user will 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

Service users will necessarily provide basic information such as contact details. In addition, Voices in Exile will be in receipt of sensitive personal data such as an individual's race, ethnic origin, politics, religion, trade union membership, physical or mental health, genetics, biometrics (where used for ID purposes), sex life or sexual orientation. This information is needed in order to provide our services to vulnerable migrants. This information is more sensitive, and therefore requires greater protection.

Whenever employees are dealing with the personal data (including photographs) of vulnerable migrants, consideration will be given to whether the data is special category data.

In the majority of cases the legal basis for processing this data will be explicit consent and this will 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 will be referred to the Director. 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 will be made to ensure that data held within the organisation is made secure (i.e. data will be anonymised / pseudonyms will be used and specific information which could identify an individual to a third party will be edited out). Photographic data is considered separately above.

Data relating to service users will be disclosed in accordance with the consent given and may also be disclosed to the Office of the Immigration Services Commissioner in accordance with our regulatory duties.

Data relating to service users will be retained for seven years after file closure.

Additional types of data

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

APPENDIX 1 - PRIVACY NOTICES

PRIVACY NOTICE FOR SUPPORTERS, PARTNERS AND EXTERNAL AGENCIES

Voices in Exile is a registered charity, number 1130363. Our mission is to help asylum seekers, refugees and vulnerable migrants and we can only achieve this with the help of our supporters and partners. We take your privacy seriously and we will deal with any personal information that you give us fairly, lawfully and transparently.

Please read this notice carefully and contact us with any questions or concerns you may have about our privacy practices.

What we need

We may collect basic information relating to our supporters and other correspondents and business contacts contacted in the course of our campaigning work. This information is likely to include your name, address, telephone numbers and email addresses. We will also collect some financial details from supporters in order to process donations.

We collect this information when you register with us, complete a contact form or during the course of doing business with us.

Voices in Exile will be what's known as the 'controller' of the information you provide to us.

How we use your personal information

We use this information to contact you, send marketing and events communications, to inform and contribute to the efficacy of our campaigning work, to comply with our legal obligations and to meet internal audit requirements.

We will, with your consent, retain your basic contact information in order to provide you with relevant updates on developments in the sector or calls to action on our campaign goals via post or email.

We may, with your consent, retain your financial details in order to facilitate any further donations you may wish to make.

We are required by our regulator to keep a list of supporters.

All the personal data we process is processed by our employees in the UK. For the purposes of IT hosting and maintenance, we have a UK-based server for back up.

If you receive marketing communications from us and no longer wish to do so, you may unsubscribe at any time by selecting the link in the email or by emailing us at administrator@voicesinexile.org.

The basis on which we use your personal information

We use your personal information on the following basis:

- To comply with legal and regulatory obligations;
- In accordance with any consent you have granted;
- Where we have a legitimate interest in that use.

How long we keep your personal information

Your personal information will be retained in accordance with our data retention policy, which categorises all the information held by us and specifies the appropriate retention period for each category of information. Those periods are based on the requirements of applicable data protection laws and the purpose for which the information is collected and used, taking into account legal and regulatory requirements to retain the information for a minimum period, limitation periods, good practice and our business purposes.

Who we share your personal information with

We may share your personal information with any entity in accordance with any consent you have given us to do so.

We may share your personal information with certain trusted third parties including:

- Our professional advisers and auditors;
- Our IT service providers;
- Third parties involved in hosting or organising events;
- Where necessary, with regulatory authorities.

We do not sell, rent or otherwise make personal information commercially available to any third party, except with your prior consent.

How we protect your personal information

We use a variety of technical and organisational measures to help protect your personal information from unauthorised access, use, disclosure, alteration or destruction consistent with applicable data protection laws.

What are your rights?

You are entitled to request details of the information we hold about you and how we process it. You may also have a right in accordance with applicable data protection law to have it rectified or deleted, to restrict or object to the processing of that information and you may withdraw any consent you have given to us. You may also have the right to lodge a complaint in relation to our processing of your personal information with the Information Commissioner's Office.

If you object to the processing of your personal information, or if you have provided your consent to processing and you later choose to withdraw it, we will respect that choice in accordance with our legal obligations.

Your objection (or withdrawal of any previously given consent) could mean that we are unable to perform the actions necessary to achieve the purposes set out above. Please note that even after you have chosen to withdraw your consent we may be able to continue to process your personal information to the extent required or otherwise permitted by law, in particular in connection with exercising and defending our legal rights or meeting our legal and regulatory obligations.

If you wish to exercise any of the rights set out in this section please email administrator@voicesinexile.org

PRIVACY NOTICE FOR SERVICE USERS

Voices in Exile is a registered charity, number 1130363. Our mission is to help asylum seekers, refugees and vulnerable migrants and we do this through the provision of immigration advice and assistance, generalist advice on welfare benefits, housing and homelessness, asylum support, children's and adult community care, foodbank and destitution service, mentoring support and group work and activities. We take your privacy seriously and we will deal with any personal information that you give us fairly, lawfully and transparently.

Please read this notice carefully and contact us with any questions or concerns you may have about our privacy practices.

What we need

In order to provide you with our services, we need some basic information such as your name, relationship to other people (for example, members of your family), contact information, financial information (for example, details of the benefits you receive) and details relating to your immigration status.

We may also need some sensitive information such as information relating to your race, ethnic origin, politics, religion, trade union membership, physical or mental health, genetics, biometrics (where used for ID purposes), sex life or sexual orientation.

We collect this information at the time you ask us for our services and during our relationship with you.

We understand that additional care may be needed when we collect and process the personal information of vulnerable people. In recognition of this, we observe good practice guidelines in our interactions with vulnerable people.

We collect information from other entities (for example the Home Office and other UK government agencies and entities, other charities, and overseas government agencies).

We collect information from entities from whom you have consented to us collecting information (for example in any consent you gave us when we first agreed to provide advice to you).

How we use your personal information

We use your personal information:

- To provide our services to you;
- To refer you to a specialist service or provider;
- To monitor and improve our performance (for example by conducting internal reviews and by providing reports on our work to our funders);
- To procure funding and other support for you (for example by preparing and submitting grant requests to other charitable bodies);
- To fulfil our legal, regulatory and risk management obligations.

All the personal data we process is processed by our employees in the UK. For the purposes of IT hosting and maintenance, we have a UK-based server for back up.

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

The legal bases under which personal information is processed by Voices in Exile caseworkers are as follows:

- Consent: you have given us clear consent for us to process your personal data for a specific purpose.
- Where we are required to process or disclose personal information to comply with legal and regulatory obligations.
- Where we have a legitimate interest in that use. Our legitimate interests in the processing of personal data are the furtherance of our campaign goals and the charitable objectives of Voices in Exile.

How long we keep your personal information

Your personal information will be retained in accordance with our data retention policy, which categorises all the information held by us and specifies the appropriate retention period for each category of information. Those periods are based on the requirements of applicable data protection laws and the purpose for which the information is collected and used, taking into account legal and regulatory requirements to retain the information for a minimum period, limitation periods, good practice and our business purposes.

Although the period varies as set out above, in general we retain personal information for at least seven years from the date of our last contact with a person. This period reflects guidance from the Office of the Immigration Services Commissioner.

Who we share your personal information with

Your personal data will be treated as strictly confidential. We will only share your data with third parties outside Voices in Exile in accordance with your consent or to meet our legal and regulatory obligations.

Your rights and your personal data

You are entitled to request details of the information we hold about you and how we process it. You may also have a right in accordance with applicable data protection law to have it corrected or deleted, to restrict or object to the processing of that information and you may withdraw any consent you have given to us. You may also have the right to lodge a complaint in relation to our handling of your personal information with the Information Commissioner's Office.

If you object to the processing of your personal information, or if you have provided your consent to processing and you later choose to withdraw it, we will respect that choice in accordance with our legal obligations.

Your objection (or withdrawal of any previously given consent) could mean that you are unable to make use of the services we offer. Please note that even after you have chosen to withdraw your consent we may be able to continue to process your personal information to the extent required or otherwise permitted by law, in particular in connection with exercising and defending our legal rights or meeting our legal and regulatory obligations.

If you wish to exercise any of the rights set out in this section please email administrator@voicesinexile.org.

APPENDIX 2 – FORM OF AUTHORITY

VOICES IN EXILE FORM OF AUTHORITY

I (name)

Date of Birth

Of (address)

Part A: storing and processing data

I authorise Voices in Exile (ViE) to store and process my personal data in a confidential manner in any database or in electronic or paper files. 'Data' may include names, addresses, details of family members, income, immigration history, national insurance and/or any other information that the worker may feel appropriate and reasonable to collect in order to proceed with my case. ViE will process this data for the purpose of providing advice to me, contacting me to let me know about services or events that may be of interest to me/my family, and for abiding by its monitoring and analysis procedures (for example internal audits and audits by external regulatory bodies such as OISC and funders).

I understand that it will be kept for a minimum of 7 years after my last contact with ViE and may then be destroyed, unless I request my data to be destroyed before this time. I understand that I have the right to see the personal data ViE holds on me, but ViE will require notice to arrange this. I understand that I can withdraw this consent at any time.

I have been given a copy of ViE's Privacy Notice and I understand that ViE's Data Protection Policy is available on request.

Signed: Date:

Part B: obtaining and disclosing data

I authorise any ViE worker to obtain and disclose relevant information on my behalf from the following organisations in order to progress my case. I understand that ViE will only obtain/disclose data in order to get the best possible outcomes for me and it may make it difficult (or impossible) for ViE workers to progress my case or support me to access services unless they can obtain/disclose data from the organisations listed below. I understand that the ViE worker will advise me further as to which organisations might be essential to progressing my case.

NHS trusts, doctor, health practitioners	☐
Home Office	☐
Government agencies (e.g. Department for Work and Pensions, Job Centre)	☐
HMRC	☐
Local authorities and social services	☐
Accommodation providers and housing trusts	☐
Voluntary sector organisations/charities/refuges	☐
Solicitors/immigration advisers/barristers	☐
School and education providers	☐
Police/ACRO criminal records office	☐
Local Member of Parliament	☐

Other (please specify) ……..	☐
Other (please specify) ……..	☐

I understand that ViE will only obtain and disclose my data if it is in my best interests and will keep me informed of disclosures that are made on my behalf. I understand that I can withdraw this consent at any time by notifying ViE.

Signed:

Date:

NB: Adults cannot sign on behalf of another adult and children who are 13 years or over must sign their own form (unless there are issues of capacity). It is not possible to consent by silence or acquiescence, so do not provide any advice to a person until they (or their parent if required) have signed this form.