# IT Security & Data Protection Policy
# Asylum Welcome

| Version Control | |
|---|---|
| Approved By | Mark Goldring |
| Version | Final |
| Policy became operational on: | May 2020 |
| Next Review Date | 30th April 2024 |
| Reviewed | April 2023 |

# Context and Overview

## Introduction

We hold personal data about our staff, volunteers, trustees, supporters, clients, suppliers and other individuals for a variety of business purposes. The aim of the IT Security & Data Protection Policy is to ensure that as a charity we comply with the requirements of EU General Data Protection Regulation (GDPR) 2016. The GDPR places a duty on us as a business to protect the personal information held on our staff and clients

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Lead be consulted before any significant new data processing activity is initiated to ensure that the relevant compliance steps are addressed.

## Definitions

| Term | Definition |
|---|---|
| Business Purposes | The purposes for which personal data may be used by us, including:<br>▪ Personnel<br>▪ Administrative<br>▪ Financial<br>▪ Regulatory<br>▪ Payroll<br>▪ Fundraising<br>▪ Business Development<br><br>*Business purposes include the following:*<br>▪ Compliance with our legal, regulatory and corporate governance obligations and good practice<br>▪ Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests<br>▪ Ensuring business policies are adhered to (such as policies covering email and internet use)<br>▪ Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information and client information, credit scoring and checking<br>▪ Investigating complaints<br>▪ Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments<br>▪ Monitoring staff conduct, disciplinary matters |

| | |
|---|---|
| | ▪ Gathering information about our clients in order to provide relevant support.<br>▪ Improving services |
| Personal Data | Any information relating to an identified or identifiable natural person ('data subject').<br><br>An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.<br><br>*Personal data we gather may include information about individuals':*<br>▪ contact details<br>▪ educational background<br>▪ financial and pay details<br>▪ qualifications, education and skills<br>▪ marital status<br>▪ Photo(s)<br>▪ job title, and CV/application form.<br>▪ Letters of Authority |
| Special Categories of Personal Data | Special categories of data include information about an individual's:<br>▪ racial or ethnic origin<br>▪ political opinions<br>▪ religious or similar beliefs<br>▪ trade union membership (or non-membership)<br>▪ physical or mental health or condition<br>▪ genetic and biometric information<br>▪ Criminal convictions, and related proceedings, are treated in the same way as special categories without<br><br>Any use of special categories of personal data should be strictly controlled in accordance with this policy. |
| Data Controller | The legal person or entity, charity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, where the purposes and means of such processing are determined by law.<br><br>Asylum Welcome is a data controller. |
| Data Processor | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.<br><br>Data processors who process data on behalf of Asylum Welcome include:<br>▪ Moneysoft Payroll Manager – processing payroll<br>▪ Intuit Quickbooks – accounts<br>▪ Donorfy – donor CRM |

| | |
|---|---|
| | ▪ Bluespires – IT support<br>▪ Computer Assistance – IT support<br>▪ Stripe – donation processing<br>▪ Computer Assistance – client database programming<br>▪ Splashtop – remote access to office computers<br>▪ Redstor – cloud backup of server<br>▪ Justgiving/CAF Donate/Stewardship<br>▪ |
| Processing | Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as:<br>▪ collection<br>▪ recording<br>▪ charity<br>▪ structuring<br>▪ storage<br>▪ adaptation or alteration<br>▪ retrieval<br>▪ consultation<br>▪ use<br>▪ disclosure by transmission<br>▪ dissemination or otherwise making available<br>▪ alignment or combination<br>▪ restriction<br>▪ erasure or destruction. |
| Supervisory Authority | The national body responsible for data protection. The supervisory authority for Asylum Welcome is the Information Commissioners Office (ICO). |

## Why this policy exists

This data protection policy ensures that Asylum Welcome:

- Complies with data protection law and follows best practice
- Protects the rights of staff, clients, supporters, trustees, volunteers and suppliers
- Is transparent about how it stores and processes individual's data
- Protects itself from the risks of a data breach.

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

## The Principles of Data Protection

Data protection is about protecting people from misuse of their personal information. Asylum Welcome regards the lawful and correct treatment of personal information as very important to successfully achieving the aims of the charity, and to maintaining stakeholder trust and confidence.

These rules apply regardless of whether data is stored electronically or on paper. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The GDPR requires that data:

1. Is processed fairly, lawfully and in a transparent manner;
2. Is collected and processed only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;
3. Is adequate, relevant and limited to what is necessary for those purposes;
4. Is accurate, up to date and not kept in an identifiable form for longer than necessary for the purposes for which it is processed.
5. Is processed in accordance with the data rights of individuals
6. Is securely held, including protection by technical and organizational measures, against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The GDPR also gives individuals the right to access, delete, correct or receive in an easily transferable format, where applicable, personal information held by the business upon request.

## Accountability and Transparency

The GDPR requires that charities demonstrate compliance with the regulation and are accountable for their use of personal data. A charity must also be transparent with individuals about how they will use the personal data they are responsible for. We will demonstrate compliance through documented plans, policies and procedures as well as maintaining an up-to-date log of our processing activities (the Information Asset Register). We will be transparent with individuals through the appropriate use of privacy information notices.

# People, Risks and Responsibilities

---

## Policy Scope

The policy applies equally to full time and part time staff on a substantive or fixed term contract, volunteers and to associated persons who work for Asylum Welcome**,** such as agency staff, contractors, trustees and others employed under a contract of service. It stipulates their duties and responsibilities for the effective handling of personal and sensitive data, in order to comply with the policy and legislative, financial and best practice requirements.

## Data Protection Risks

This policy helps to protect Asylum Welcome from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the charity uses data relating to them.
- **Reputational damage.** For instance, the charity could suffer if hackers successfully gained access to sensitive data.
- **Financial damage.** For instance, if a significant personal data breach were to occur the ICO may impose a substantial financial penalty on the organization.

## Data Controller

The GDPR determines the role of a Data Controller as a 'legal' person or company that determines the purposes and means of any personal information and is fully responsible for the actions of anyone processing data on behalf of the charity. The **Data Protection Lead is** the Director.

## Responsibilities

Everyone who works for or with Asylum Welcome must process personal data fairly and lawfully in accordance with individuals' rights.

Each member of staff that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibilities:

- The Board of Trustees is ultimately responsible for ensuring that Asylum Welcome meets its legal obligations.

- The Finance & Contracts manager will fulfil the role of **Data Protection Lead**. The **Data Protection Lead,** is responsible for:

    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals such as clients and staff to see the data Asylum Welcome holds about them (also called Subject Access Requests).
    - Checking and approving any contracts or agreements with third parties that may handle the charity's sensitive data.
    - Leading on responding to and managing a data protection breach
    - Liaising with the ICO to report and investigate personal data breaches if required.

- The Office Manager will fulfil the role of **IT Manager.** The IT Manager, is responsible for:

- ensuring that all IT Systems are assessed and deemed suitable for compliance with the Charity's security requirements;
- ensuring that IT security standards within the Charity are effectively implemented and regularly reviewed, working in consultation with the Charity's senior management and Data Protection Lead (as appropriate), and reporting the outcome of such reviews to the Charity's senior management, and where appropriate with the Board of Trustees;
- ensuring that all Users are kept aware of the requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the GDPR and the Computer Misuse Act 1990.
- assisting all Users in understanding and complying with this Policy;
- ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, considering their job role, responsibilities, and any special security requirements;
- receiving and handling all reports relating to IT security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the Data Protection Lead;
- taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;
- monitoring all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future; and
- ensuring that regular backups are taken of all data stored within the IT Systems at intervals no less than daily and that such backups are stored on the Redstor Cloud server. All backups should be encrypted.

• **The Director** will fulfil the role of **Marketing Manager.** The **Marketing Manager,** is responsible for:

- Approving any data protection privacy statements attached to communications such as emails and letters, in conjunction with the Data Protection Lead.
- Addressing any data protection queries from clients, target audience, journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Ensuring that only personal data with the appropriate legal basis for processing for marketing activities is used

# General Staff Guidelines

---

- All Users must comply with all relevant parts of this Policy at all times when using the IT Systems and processing personal data.

- All Users must use the IT Systems and process personal data only within the bounds of UK law and must not use the IT Systems or personal data for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.

- Users must immediately inform the IT Department and, where such concerns relate to personal data, the Data Protection Lead) of any and all security concerns relating to the IT Systems or breaches of personal data.

- Users must immediately inform the IT Department of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.

- Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Charity's disciplinary procedures.

- The only people able to access data covered by this policy should be those who need it for their work (please refer to Information Asset Register)**.**

- Personal Data should not be shared informally. When access to confidential information is required, staff can request it from their line manager.

- Asylum Welcome will provide training to all staff, and where appropriate to volunteers and trustees to help them understand their responsibilities when handling personal data.

- Staff should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong passwords must be used and they must never be shared. They must not be stored centrally.

- Personal data must not be disclosed to unauthorised people, either within the charity or externally.

- Data must be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of (please refer to the retention periods set out in the Information Asset Register).

- Staff must request help from the Data Protection Lead if they are unsure about any aspect of data protection.

# Our Procedures

---

## Fair and lawful processing

Asylum Welcome must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. If we cannot apply a lawful basis as outlined below, our processing does not conform to the first principle and will be unlawful. Individuals have the right to have any data unlawfully processed erased. We will ensure that any new

processing activities are assessed with a privacy by design approach prior to undertaking the processing. The following procedure will ensure that we meet this requirement of the regulation.

## Lawful basis for processing data

Asylum Welcome must establish a lawful basis for processing data. Staff must ensure that any data they are responsible for managing has a documented lawful basis approved by the Data Protection Lead in the information asset register. It is each employee's responsibility to check the lawful basis for any data they are working with and ensure all of their actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent:** We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract:** The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation:** We have a legal obligation to process the data (excluding a contract).

4. **Vital interests:** Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public function:** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest:** The processing is necessary for our legitimate interests, and does not outweigh the individual's rights.

## Deciding which condition to rely on

When Asylum Welcome are making an assessment of the lawful basis, we will first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We cannot rely on a lawful basis if we can reasonably achieve the same purpose by some other means.

Where more than one lawful basis applies, Asylum Welcome will rely on what will best fit the purpose, not what is easiest.

We will always consider the following factors and document the answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Asylum Welcome's commitment to accountability and transparency requires that we document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This will be achieved via a privacy information notice. This applies whether we have collected the data directly from the individual, or from another source.

Staff who are responsible for assessing the lawful basis and implementing the privacy notice for new processing activities must have them approved by the **Data Protection Lead**.

# IT Security

This section sets out the measures to be taken by all staff, volunteers and trustees of Asylum Welcome and by the Charity as a whole in order to protect the Charity's computer systems, devices, infrastructure, computing environment and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate, or accidental.

### Software Security Measures

- All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases will be applied at the sole discretion of the IT Department. Unless a software update is available free of charge it will be classed as a major release, falling within the remit of new software procurement and outside the scope of this provision.

- Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied. If the security flaw affects, is likely to affect, or is suspected to affect any personal data, the Data Protection Lead shall be informed immediately.

- Employee cannot install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the IT Manager. Any software belonging to an employee must be approved by the IT Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

- All software will be installed onto the IT Systems by the IT Department unless an individual user is given written permission to do so by the IT Manager. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

**Anti-Virus Security Measures**

- Most IT Systems will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up-to-date with the latest software updates and definitions.

- All IT Systems protected by anti-virus software will be subject to a full system scan at least daily.
- All physical media (e.g. USB memory sticks or disks of any kind) used by staff for transferring files must be virus-scanned before any files may be transferred.

- Staff shall be permitted to transfer files using cloud storage systems only with the approval of the IT Manager. All files downloaded from any cloud storage system must be scanned for viruses during the download process.

- Any files being sent to third parties outside the Charity, whether by email, on physical media, or by other means (e.g. shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate.

- Where any virus is detected by staff this must be reported immediately to the IT Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device.

- If any virus or other malware affects, is likely to affect, or is suspected to affect any personal data, in addition to the above, the issue must be reported immediately to the Data Protection Lead.

- Where any staff deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company’s disciplinary procedures.

## Hardware Security Measures

- Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised staff being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, staff must not allow any unauthorised access to such locations for any reason.

- All IT Systems not intended for normal use by staff (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by designated members of the IT Department.

- No staff shall have access to any IT Systems not intended for normal use by staff (including such devices mentioned above) without the express permission of the IT Manager. Under normal circumstances, whenever a problem with such IT Systems is identified by a staff, that problem must be reported to the IT Department. Under no circumstances should staff attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the IT Manager.

- All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.

- All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Charity should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Staff should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or Company premises. If any such mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment.

- The IT Department shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled, and the corresponding data shall be kept on the asset register.

## Access Security

- Access privileges for all IT Systems shall be determined on the basis of Users' levels of authority within the Charity and the requirements of their job roles. Users shall not be granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.

- All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system as the IT Department may deem appropriate

and approve. Not all forms of biometric log-in are considered secure. Only those methods approved by the IT Department may be used.

- All passwords must, where the software, computer, or device allows:
  - be at least 8 characters long;
  - contain a combination of upper case & lower case letters, numbers and symbols;
  - rather than insisting passwords are changed at regular intervals, we should ensure that different passwords are used for different systems and if possible changed annually.
  - be different from the previous password;
  - not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.); and
  - be created by individual Users.

- Passwords should be kept secret by each staff member. Under no circumstances should staff share their password with anyone, excluding the IT Manager and the IT Staff. No staff member will be legitimately asked for their password by anyone at any time and any such request should be refused. If a staff member has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to the IT Department and, where personal data could be accessed by an unauthorised individual, the Data Protection Lead.

- If a member of staff forgets their password, this should be reported to the IT Department. The IT Department will take the necessary steps to restore the staff member's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.

- Users should not write down passwords if it is possible to remember them. If a User cannot remember a password, it should be stored securely (e.g. in a locked drawer or in a secure password database) and under no circumstances should passwords be left on display for others to see (e.g. by attaching a note to a computer display).

- All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after a period of inactivity. This time period cannot be changed by staff and staff may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).

- All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Charity shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake, or similar. Users may not alter this time period.

- Staff may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Manager. Any such software must be reasonably required by the member of staff for the performance of their job role and must be fully inspected and cleared by the IT Manager and, where such access renders personal data accessible by the outside party, the Data Protection Lead.

## Data Storage Security

- All data, and in particular personal data, should be stored securely using passwords and data encryption.

- All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Charity or otherwise without the formal written approval of the Data Protection lead and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

- No data, and in particular personal data, should be transferred to any computer or device personally belonging to an employee, volunteer or trustee unless the individual in question is a contractor or sub-contractor working on behalf of the Charity and that individual has agreed to comply fully with this policy.

- Staff must not work on confidential or personal data in public areas (e.g. cafes or public transport) where there is a high risk of information being seen by other people nearby. If mobile working is necessary, the Data Protection Lead can provide additional security measures to protect the information so it cannot be seen (e.g. screen protectors for laptops or tablets).

- Staff must consider their location when talking on the phone or meeting with clients when discussing personal or confidential details. The reception area, public places and public transport are not suitable locations to hold confidential conversations.

## Data Accuracy and Relevance

Asylum Welcome will ensure that any personal data that is processed is accurate, adequate and relevant and not excessive, given the purpose for which it is obtained. Asylum Welcome will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

It is the responsibility of all staff who work with personal and or personal sensitive data to take reasonable steps to ensure it is kept accurate and up to data as possible.

- Data will be held in as few places as necessary. Staff must not create any unnecessary additional data sets. Please see information asset register for the complete list of information assets and where they are stored.

- Staff will take every opportunity to ensure that data is updated. For instance, by confirming a client's details when they call.

- If an individual identifies that personal data held by Asylum Welcome is inaccurate and requests that the charity updates the information, the charity will review the data and make the appropriate updates without undue delay and within 30 days.

- Staff must take reasonable steps to ensure that personal data that Asylum Welcome holds on them is accurate and updated as required, for example if their personal circumstances change or they change address.

## Data Audit and Register

Regular data audits to manage and mitigate risks will inform the information asset register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. It will be reviewed on a regular basis and at a minimum annually, or when the charity undertakes new data processing.

# Individuals' Rights

---

Asylum Welcome will ensure any use of personal data is justified using at least one of the conditions (e.g. consent, legitimate interest, performance of a contract, legal obligation) for processing and this will be specifically documented within the Information Asset Register. All staff that are responsible for processing personal data will be aware of the conditions for processing. The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

## Subject Access Requests

All individuals who are the subject of personal data held by Asylum Welcome are entitled to:

- Ask **what information** the charity holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the charity is **meeting its data protection obligations**.

If an individual contacts the charity requesting this information, this is called a subject access request.

Subject access requests from individuals can be made by email, addressed to the Data Protection Lead at office@asylum-welcome.org or in writing to: Data Protection Lead, Asylum Welcome, Unit 7 Newtec Place, Magdalen Road, Oxford OX4 1RE. Asylum Welcome may supply a standard request form, although individuals do not have to use this. If a subject access request is sent directly to another Asylum Welcome employee, they must pass it immediately to the Data Protection Lead to handle.

The Data Protection Lead will always verify the identity of anyone making a subject access request before handing over any information. One of the following forms of ID will be required:

- Passport
- Photocard Driving Licence

Asylum Welcome will aim to provide the relevant data without delay, and certainly within 30 days. Where the request is more complex, we will notify the individual making the request of any likely delay and extension period required

## Right to Erasure

In certain circumstances, an individual may request that any information held on them by Asylum Welcome is deleted or removed, and any third parties who process or use that data must also comply with the request.

An individual has the right to have their information erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for
- the legal basis on which the charity is holding the personal data is consent, and the individual withdraws their consent
- the legal basis on which the charity is processing the data is legitimate interests, and the individual objects to the processing of that data, and the charity is unable to demonstrate that overriding legitimate interests to continue this processing exists
- the charity have processed the personal data unlawfully
- the charity must delete the data in order to comply with a legal obligation

An individual does not have the right to have their information erased if the processing of their personal data by Asylum Welcome is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for the establishment, exercise or defence of legal claims

Requests from individuals can be made by email, addressed to the Data Protection Lead at office@asylum-welcome.org or in writing to: Data Protection Lead, Asylum Welcome, Unit

7 Newtec Place, Magdalen Road, Oxford OX4 1RE. They may also make the request verbally in person or via telephone: 01865 722082.

Asylum Welcome will aim to provide the relevant data without delay, and certainly within 30 days. Where the request is more complex, the Data Protection Lead will notify the individual making the request of any likely delay and extension period required.

In the event that any personal data that is to be erased in response to an individual's request has been disclosed to third parties, the Data Protection Lead will inform those parties of the erasure (unless it is impossible or would require disproportionate effort to do so).

# Data Breaches

Any data breach of personal information must be recorded by Asylum Welcome**.** The GDPR sets out the requirements to respond to a personal data breach.

- Data controllers (Asylum Welcome) must report certain types of data breach to the supervisory authority (Information Commissioners Officer (ICO)) without undue delay and within 72 hours or becoming aware of data breach.

- Data controllers will be required to notify individuals affected by the data breach in circumstances where it is likely to cause a high risk to their rights and freedoms.

- A breach notification to the ICO should include:
  - The nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned; and
    - Categories and approximate number of personal data records concerned;

  - The name and contact details of the Data Protection Lead.

  - A description of the likely consequences of the personal data breach.

  - A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measure taken to mitigate any possible adverse effects.

In order to effectively monitor data breaches, the Data Protection Lead will document each data breach in the Asylum Welcome Data Breach Log file, including facts of the breach, the effects and action taken. The Data Protection Lead, with relevant support from staff in the organization, will assess the likely risk and impact on individuals affected by the breach immediately, and where necessary report to the ICO within 72 hours via the ICO website. Further details about the breach will be established using the data breach process.

### Data Breach Process

In order to understand why a breach occurred and prevent further breaches, the Data Protection Lead will:

- Determine how the breach happened.
- Determine what, if anything, could have been done to prevent it.
- Understand what can be done to prevent future breaches.
- Determine how soon the changes can be implemented
- Update and cascade training for staff as soon as possible
- Provide an update to individuals affected by the breach on the outcome of the investigation and what we are doing to prevent future breaches
- Provide an update to the Partnership Board on the outcome of the investigation and what we are doing to prevent future breaches
- Deal with any complaints
- Respond to any requests for further information from the Information Commissioner's Office (*if relevant*).
- implement and comply with recommendations from the Information Commissioner's Officer.

## Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, Asylum Welcome will disclose requested data. However, the Data Protection Lead will ensure the request is legitimate, seeking assistance from the board and from the charity's legal advisers where necessary

## Policy Compliance

If any user is found to have breached this policy, they may be subject to Asylum Welcome's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Any unauthorised disclosure of personal data to a third party by an employee will be viewed seriously and may result in disciplinary proceedings.

The Board of Trustees are accountable for compliance of this policy. A director could be personally liable for any penalty arising from a breach that they have made.