Data Protection Policy

Last updated: July 2018

1. About this policy

The Welcoming is committed to ensuring good practice in its handling and storage of personal data. This is in order to meet the requirements of the current data protection legislation of the UK, and to protect the rights of employees, volunteers, service users and members of the public including taking all necessary steps to protect their personal data from data security breaches.

In order to carry out its charitable activities, the Welcoming needs to gather and use information about individuals. This policy describes how this data will be collected, handled and stored to meet the organisation's data protection standards and to comply with the law.

2. Data Protection Law

The current data protection legislation describes how organisations must collect, handle and store personal information. These rules apply to personal data stored in a permanent format either electronically or non-electronically.

To comply with the law, the Welcoming must process personal data in accordance with the six Data Protection Principles set out in the current data protection legislation. These say that personal data must:

1. Be processed fairly and lawfully

2. Be obtained only for specific, lawful purposes

3. Be adequate, relevant and not excessive

4. Be accurate and kept up to date

5. Not be held for any longer than necessary

6. Be protected and kept secure in appropriate ways

The legislation also specifies that organisations are required to take responsibility for complying with the principles and to have appropriate processes and records in place to demonstrate compliance.

3. Responsibilities

This policy applies to all Welcoming employees and volunteers, and all contractors, suppliers and other people working on behalf of the Welcoming.

It applies to all data that the Welcoming holds relating to identifiable individuals, which can include, but is not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Images of identifiable individuals (including photos and video)
- Sensitive personal data (including information relating to physical or mental health, ethnicity, sexuality, faith etc.)
- Other information relating to individuals as required

Everyone who works for or with the Welcoming has some responsibility for ensuring data is collected, stored and handled appropriately.

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

The Co-Directors, on behalf of the Welcoming Board, have overall responsibility for ensuring that the Welcoming meets its legal obligations, including:

- Reviewing all data protection procedures and related policies as and when needed, and at least every 12 months.
- Ensuring that there is adequate security in place for all physical materials
- Ensuring that there is adequate IT security in place, liaising with the Welcoming's IT support providers to ensure that all IT systems, services and equipment used for processing data meet acceptable security standards.
- Ensuring that staff, volunteers and contractors are appropriately trained in their responsibilities.
- Arranging data protection training and advice for employees and volunteers.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the Welcoming holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data and/or personal data.
- Approving any data protection statements attached to communications such as activity forms, emails and letters.
- Evaluating any third-party services the company is considering using to store or process sensitive data and/or personal data. For instance, cloud computing services.

4. General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their current role at the Welcoming.
- Personal data should not be shared informally.
- The Welcoming will provide initial and refresher training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong passwords must be used and they should never be shared. Guidance on how to create a strong password will be issued to all staff.
- All electronic devices must be password-protected or encrypted, including mobile phones, USB memory sticks and portable hard drives.
- Personal data should not be disclosed to unauthorised people, either within the organisation or externally.
- Staff should be aware of the possibilities of people overhearing discussions about individuals in the shared office/reception/meeting spaces at the Welcoming.
- Confidential meeting space should be booked for occasions where details about individuals are likely to be discussed.
- Data should 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 securely.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.

5. Data collection

These rules describe the principles and procedures that should be followed when collecting personal data from individuals.

- When collecting personal data (which includes images such as photos or videos of identifiable individuals), the subject must always be informed of the purpose for which the data is being collected and how it will be used.
- The data subject should always give their informed consent before data is collected. This consent should ideally be given in writing, or details recorded by the data collector if given verbally.
- When collecting data on subjects under the age of 12, parental consent must be obtained in all circumstances by a signed consent form, letter or email. Where this consent has been collected by a third party (such as a school), a copy of the consent should be kept on file.

6. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to a Co-Director.

Data should always be stored only for as long as it is needed and must be disposed of securely (eg by shredding) when no longer required.

6.1 Paper Data Storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, confidential material should be kept in a locked drawer or filing cabinet in the main Welcoming office.
- Employees should make sure paper and printouts containing confidential information are not left where unauthorised people could see them, such as on a printer.
- Employees should only print documents when they know they can collect them straight away.
- Data printouts should be shredded and disposed of securely when no longer required.

- The office where physical data is stored should have a high level of security, the external doors to be kept locked at all times, and keys only to be issued to employees and sessional staff who have received a full Welcoming staff induction.

6.2. Electronic Data Storage

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed at least every 3 months and never shared between employees.
- If data is stored on removable media (e.g. a CD or USB memory stick), these should be encrypted and kept locked away securely when not being used.
- Data should only be stored on the cloud computing services that have been approved by the Welcoming.
- Work-related personal data should never be saved directly to personal or work laptops or other mobile devices like tablets or smart phones.
- All computers containing data should be protected by approved security software.

7. Data use

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should never be sent to third parties or external contacts unless the subject has given explicit consent to do so.
- Employees should never save copies of personal data to their own personal or work computers, but should instead always access and update the central copy on Office 365.

8. Data accuracy

The law requires the organisation to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the Welcoming will put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary.
- Staff should not create any unnecessary additional data sets.
- The Welcoming will endeavour to reduce duplication of personal data by creating and using central databases and contact lists wherever possible.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a contact's details if they get in touch with the Welcoming after a period without contact.
- Data should be updated as inaccuracies are discovered. For instance, if an email bounces or a contact can no longer be reached on their stored telephone number, it should be removed from the relevant list or database.

9. Subject access request

All individuals who are the subject of personal data held by the Welcoming are entitled by law to:

- Ask what information the company holds about them and why.
- Request a copy of the data in a permanent format.

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

Subject access requests from individuals must be made in a permanent format eg by email or post, addressed to the Welcoming. Consideration will be given to circumstances where this is not possible.

Individuals will be charged £10 per subject access request. The Welcoming will aim to provide the relevant data within 14 days or at the latest by the timescale specified in the current data protection legislation.

The Welcoming will always verify the identity of anyone making a subject access request before handing over any information.

10. Disclosing data for other reasons

In certain circumstances, data protection legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances the Welcoming will disclose the requested data providing they are satisfied that the request is legitimate. They will seek assistance from the Board of Directors and from the Welcoming's legal advisers where necessary.