The Ashdown Forest Foundation – Data Protection Policy

Overview

Under the UK General Data Protection Regulation 2016 (UK GDPR) The Ashdown Forest Foundation (Charity) is required to comply with the UK GDPR and undertakes to do so. The UK GDPR sits alongside an amended version of the Data Protect Act 2018.

The UK GDPR describes how organisations need to gather and use certain information about individuals. This regulation applies regardless of whether data is stored electronically, on paper or on other materials.

The Charity need to gather and use certain information about individuals. Such individuals can include donors, suppliers, business contracts, Charity partners and other people the Charity has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Charity's data protection standards and to comply with the law.

This policy ensures the Charity:

1. Complies with data protection law and follows good practice
2. Protects the rights of the Board of Trustees, staff, volunteers and individuals representing the Charity
3. Is transparent about how it processes and stores personal information.

1. Policy Scope

This policy applies to:

- All trustees, staff, volunteers and individuals working on behalf of the Charity
- All contractors, suppliers and other people working on behalf of the Charity

It applies to all data and personal information that the Charity holds relating to identifiable individuals, even if that information technically falls outside of the UK GDPR. This can include:

- full name (including any preferences about how they like to be called)
- full postal address
- telephone and/or mobile number(s)
- e-mail address(es)
- social media IDs/UserNames (eg: Facebook, Skype, Hangouts, WhatsApp)

2. Key Definitions[1]

The UK GDPR applies to 'controllers' and 'processors'.

- If you are a processor, the UK GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach

- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the UK GDPR places further obligations on you to ensure your contracts with processors comply with the UK GDPR

- The UK GDPR applies to processing carried out by organisations operating within the UK. It also applies to organisations outside the UK that offer goods or services to individuals in the UK
- The UK GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Data Protection Officer

The primary role of the data protection officer (DPO) is to ensure that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. The Data Protection Officer on behalf of the Charity is the Charity Administrator.

Data Controller

A controller determines the purposes and means of processing personal data. For the purpose of this policy, the Charity Administrator is the Data Controller on behalf of the Charity.

Data Processor

A processor is responsible for processing personal data on behalf of a controller. For the purpose of this policy the Charity Administrator is the Data Processors on behalf of the Charity.

[1] Key definitions | ICO

Data Subject

A data subject is an identifiable individual person about whom the Charity holds personal data.

3. General Principles[2]

To comply with the law, personal information must be collected and used fairly, stored safely and not be disclosed unlawfully. The UK GDPR is underpinned by 7 principles:

1. Lawfulness, fairness and transparency
   Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

2. Purpose limitation
   Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

3. Data minimisation
   Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4. Accuracy
   Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5. Storage limitation
   Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

6. Integrity and confidentiality (security)
   Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

7. Accountability
   The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

[2] https://www.gov.uk/data-protection

The Charity is required to take responsibility for what it does with personal data and how it complies with the other principles. The Charity is required to have measures and records in place to demonstrate compliance to UK GDPR.

4. Responsibilities

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

The Data Controller is responsible for:

1) Keeping the trustees, staff, volunteers and individuals working on behalf of the Charity updated about data protection responsibilities, risks and issues
2) Reviewing, in conjunction with the trustees, all data protection procedures and related policies
3) Arranging data protection training and advice for the people covered by this policy where applicable
4) Handling data protection questions covered by this policy
5) Dealing with requests from individuals and donors to see the data held by the Charity (also called 'subject access requests')
6) Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data. For instance, cloud computing services
7) Registering (where applicable) and notifying (where applicable) the Information Commissioner's Office (ICO) of the data it holds or is likely to hold, and general purposes that this data will be used for
8) Approving any data protection statements attached to communications such as emails and letters.
9) Addressing any data protection queries from journalists or media outlets like newspapers
10) Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

5. Data Protection Risks

This policy helps to protect the Charity and individuals from some very real data security risks, including:

1) Loss or unavailability of personal information. For instance data storage method being lost or made inaccessible
2) Breaches of confidentiality. For instance, information being given out inappropriately
3) Reputational damage. For instance, the Charity could suffer if hackers successfully gained access to sensitive data.

6. Lawful Processing

The Charity will obtain, hold and process all personal data in accordance with the UK GDPR for the following lawful purposes.

1. <u>By Consent</u>

The information collected may additionally contain details of any particular areas of interest about which the person wishes to be kept informed. The information provided will be held and processed solely for the purpose of providing the information requested by the person.

2. By Contract
   People who sell goods and/or services to, and/or purchase goods and/or services from the Charity. The information collected will additionally contain details of:

   The information provided will be held and processed solely for the purpose of managing the contract between the Charity and the person for the supply or purchase of goods/services.

3. For Legitimate Interest, e.g. Volunteers, including Trustees
   In order to be able to operate efficiently, effectively and economically, it is in the legitimate interests of the Charity to hold such personal information on its trustees, staff, volunteers and individuals working on behalf of the Charity to enable the Charity to communicate on matters relating to the operation of the charity, for example:
   I. the holding of meetings;
   II. providing information about the Charity's activities –particularly those activities which, by their nature, are likely to be of particular interest to individual volunteers/trustees;
   III. seeking help, support and advice from volunteers/trustees, particularly where they have specific knowledge and experience;
   IV. ensuring that any particular needs of the volunteer/trustee are appropriately and sensitively accommodated when organising meetings and other activities of the Charity;
   V. In the case of data obtained directly from the data subject, the information will be provided at the time the data are obtained.

7. Access to Data

Except where necessary to pursue the legitimate purposes of the Charity, only the Data Processors shall have access to the personal data held by the Charity.

8. Collecting Personal Data

The Charity collects a variety of personal data commensurate with the variety of purposes for which the data are required in the pursuit of its charitable objects.

All personal data will be collected, held and processed in accordance with the relevant Data Privacy Notice provided to data subjects as part of the process of collecting the data.

A Data Privacy Notice will be provided, or otherwise made accessible, to all persons on whom the Charity collects, holds and processes data covered by the UK GDPR. The Data Privacy Notice provided to data subjects will detail the nature of the data being collected, the purpose(s) for which the data are being collected and the subjects rights in relation to the Charity's use of the data and other relevant information in compliance with the prevailing UK GDPR requirements.

9. Data Processing

Data Processors shall only process the Charity's personal data in a secure location and not in any public place, eg: locations whether the data could be overlooked by others, or the removable data storage devices would be susceptible to loss or theft. Computers/laptops in use for data processing will not be left unattended at any time.

10. Data storage

The Charity regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom the Charity work. The Charity intends to ensure that personal information is treated lawfully and correctly.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. Whenever possible the secure place should be a locked filing cabinet, ideally kept in a room which is also locked when unattended.

However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

1) When working with personal data, trustees should ensure the screens of their computers computers and other devices are always locked when left unattended
2) Workstations must be protected by a password protected screensaver that automatically triggers after 5 minutes of inactivity
3) Personal data should not be shared informally verbally or electronically. Care should be taken to avoid sending bulk details by email
4) Personal information must be accessed only for approved business purposes and on a "need to know" basis and should not be printed, copied or otherwise reproduced
5) Data shall not be transferred to a country or territory outside the European Economic Area
6) Printers should be switched off and locked outside working hours. Printed materials containing personal information must be collected immediately by the originator
7) Incoming and outgoing mail collection points must be supervised so that letters cannot be stolen or lost
8) When not required, the paper or files should be kept in a locked drawer or filing cabinet
9) Trustees, staff and volunteers of the Charity who have access to personal data should make sure paper and printouts are not left where unauthorised people could see them, like on a printer
10) Printed personal data should be shredded and disposed of securely when no longer required
11) Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service
12) Servers containing personal data should be sited in a secure location
13) Data should be backed up frequently
14) All servers and computers containing data should be protected by approved security software and a firewall.

11. Data Accuracy

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

It is the responsibility of all trustees 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. Trustees should not create any unnecessary additional data sets. For example; when sending data via email, whenever possible send a hyperlink rather than attach a document which will prevent multiple copies of the data being created.

Trustees should take every opportunity to ensure data is updated. For instance, by confirming a donor's details when they meet with them.

Data should be updated as inaccuracies are discovered and the correct data verified. For instance, if a commoner or resident can no longer be reached on their stored telephone number, the new number should be verified and recorded and the old number should be removed from the database.

12. Data Breach Reporting Plan

In the event of any data breach coming to the attention of the Data Controller, whether actual or suspected, the breach will be fully investigated by the Data Controller within such a timeframe as to enable reporting to the ICO within 72 hours (if required).

In the event that full details of the nature and consequences of the data breach are not immediately accessible (eg: because Data Processors do not work on every normal weekday) the Data Controller will bring that to the attention of the ICO and undertake to forward the relevant information as soon as it becomes available.

The Charity takes its responsibilities for the security of personal information very seriously and will take all reasonable steps to ensure personal data is processed securely and remains available upon request. The following would constitute a data breach:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction)
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Following investigation, the following decisions will be made and acted on.

1. Is the breach likely to result in a high risk to the rights and freedoms of individuals?
2. Is the Charity required to report the incident to the ICO?
3. Does the Charity need to contact the individual's affected?
4. What steps, if any, can the Charity take to mitigate or minimise the impact of the data breach?
5. What steps can the Charity take to prevent reoccurrence?

A log of actual and suspected data breaches will be maintained by the Data Controller and be made available for discussion and review upon request.

13. Subject Access Requests

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

1. Ask what information the company holds about them and why
2. Ask how to gain access to it
3. Be informed how to keep it up to date
4. Be informed how the company 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 should be made by email, addressed to the Data Controller at the following address:

The Data Controller
The Ashdown Forest Foundation

The Ashdown Forest Centre
Wych Cross
Forest Row
RH18 5JP
hello@ashdownforestfdn.org

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

14. Data Subjects[3]

Under the Data Protection legislation, data subjects have the following rights with regards to their personal information:

1) The right to be informed
2) The right of access
3) The right to rectification
4) The right to erasure
5) The right to restrict processing
6) The right to data portability
7) The right to object
8) Rights in relation to automated decision making and profiling

It will be explained to subjects who make a request to access their data and/or to have errors or omissions corrected, or that their data be erased, that, while their requests will be actioned as soon as is practical there may be delays where the appropriate trustees, staff or volunteers of the Charity do not work on every normal weekday.

Where a data subject requests that their data be rectified or erased the Data Controller will ensure that the rectifications or erasure will be applied to all copies of the subject's personal data.

15. Disclosing data for other reasons

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

Under these circumstances, the Charity will disclose requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from legal advisers where necessary.

The Charity will not knowingly outsource its data processing to any third party.

Date of Policy	August 2022
Policy Review Date	
Policy approved by	The Board of Trustees

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/individual-rights/

16. Definitions

Please find below definitions of some of the terms used in this Privacy Policy for your information and assistance.

Processing

"processing" means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data, retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission,
- dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

Personal Data

Personal data is:

- any data from which the identity of a living individual can be determined, either by itself or with other data processed by data controller;
- any information such as name and address, email address, telephone number and general contact details, personal data includes images on film (e.g. CCTV images), photographs and telephone voice recordings.

Contact Information

For the purposes of this Policy, "Contact Information" means any or all of the person's:

- full name (including any preferences about how they like to be called)
- full postal address
- telephone and/or mobile number(s)
- e-mail address(es)
- social media IDs/UserNames (eg: Facebook, Skype, Hangouts, WhatsApp)

Special Categories of Personal Data

Special Categories of Personal Data means personal data consisting of information as to:

- the racial or ethnic origin of the data subject;
- the data subject's political opinion;
- the data subject's religious beliefs or other beliefs of a similar nature;
- whether the data subject is a member of a trade union; genetics;
- biometrics (where used for ID purposes);
- the data subject's physical or mental health or condition; or
- the data subject's sexual life or sexual orientation.