Data Protection and Information Security Policy

Actcessible is committed to protecting the privacy and personal data of all individuals with whom we work.

We collect, store, and process information about our service users, employees, freelancers, donors, and other stakeholders in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy outlines how we manage personal data securely, lawfully, and transparently.

Purpose of this Policy

This policy is intended to:

- Ensure compliance with data protection legislation
- Protect the rights of individuals
- Provide a clear framework for managing data and upholding confidentiality
- Outline procedures for handling data breaches and access requests

Scope

This policy applies to all trustees, employees, volunteers, freelancers, and third-party contractors who have access to personal data collected or held by Actcessible.

Definition of personal data

Personal data is any information that relates to an identified or identifiable living individual. This means that the information can be used, either directly or indirectly, to identify a specific person. Examples include names, addresses, telephone numbers, email addresses, identification numbers, donation history, volunteer and staff application details, beneficiary records (e.g. service users), etc. and online identifiers like IP addresses. It also includes less obvious information that, when combined with other data, could lead to identifying a person, such as birthdates, postal codes, and even browsing history.

Direct identifiers:

These are pieces of information that can directly identify an individual, such as a name, a social security (National Insurance) number, or a passport number. Actcessible may need these for payroll processing, volunteer contact, identification & payment of expenses for instance.

Indirect identifiers:

These are pieces of information that, on their own, might not identify someone, but when combined with other information, can lead to identification. Examples include birthdates, postal codes, job titles, and even browsing history. Actcessible may need to use Indirect identifiers for payroll processing, volunteer contact, identification & payment of expenses for instance.

Online identifiers:

In the digital age, online identifiers like IP addresses, cookie IDs, and device IDs are also considered personal data. Such personal data may be collected by Actcessible when reviewing website interactions, for example. A recorded audition may include an actor's voice or image and would therefore be used to directly identify an individual. Actcessible include this under the definition of personal data.

Data that can be combined:

Information that might not identify someone on its own, but when combined with other information, can reveal an individual's identity, also constitutes personal data. An example would be if Actcessible received a feedback poll that categorized respondents within age brackets and only one individual was in that bracket.

Images:

An image is considered personal data if it contains information that can be used to identify a living individual.

This could be a photograph or video where the person is named or where other contextual information (like a caption or location) allows for identification.

Even images of small groups or crowds can be personal data if the individuals within the image can be identified.

Actcessible will use images for various purposes, but only with the specific written consent of any individual in the image, or their parent/guardian and only for the specific purpose(s) stipulated. Actcessible will review all images to determine if they are potentially to be classified as personal data and therefore to be treated as such.

Voice Recordings:

Voice recordings are also considered personal data if they contain information that can be used to identify an individual.

This includes the content of the recording, as well as characteristics like tone, pitch, accent, and rhythm, which can be used to identify a person.

Voice recordings can also reveal sensitive information like ethnic origin or health conditions, which are subject to even more stringent protections under data protection laws.

Why the definition of personal data is important

The concept of personal data is central to data protection laws and regulations like the GDPR, which aim to safeguard individuals' rights and ensure responsible handling of their information.

Legal Framework

We are guided by the following principles of data protection under the UK GDPR:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Roles and Responsibilities

- Actcessible will appoint a designated Data Protection Lead (DPL) responsible for ensuring compliance and reporting any breaches. David Owen (Trustee) was appointed as the DPL on 22/07/2025. Kyle Lewis Illsley was appointed as the Deputy DPL on 22/07/2025.
- All individuals handling personal data must adhere to this policy and complete relevant training.
- Project leads are responsible for ensuring data protection is considered in project planning, data collection and reporting.

Collecting and Using Personal Data

We collect personal data to:

- Communicate with participants and stakeholders
- Deliver our charitable services and activities

- Recruit and manage staff and volunteers
- Meet contractual, legal, and safeguarding obligations
- Fundraise and report to donors

We will:

- Only collect the minimum amount of data required
- Use data only for the purpose it was collected
- Clearly inform individuals why and how their data will be used
- Obtain explicit consent where required

Lawful Processing

Actcessible is committed to processing personal data lawfully, fairly, and transparently in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The charity identifies a lawful basis for all data it collects, holds, and processes. The lawful bases relevant to Actcessible's operations are as follows:

1. Consent

The individual has given clear and informed consent for Actcessible to process their personal data for a specific purpose. This includes, for example, signing up to receive newsletters, marketing updates, or digital resources. Consent will always be freely given, specific, informed, and unambiguous, and individuals will have the right to withdraw their consent at any time. Actcessible will never share personal data with third parties for marketing purposes without explicit consent.

2. Contractual Obligation

Processing is necessary for a contract with the individual or to take steps at their request before entering into a contract. This includes, for example, processing data to issue volunteer agreements, freelance contracts, or confirming bookings for Actcessible's performances or workshops.

3. Legal Obligation

Processing is necessary for compliance with a legal obligation. This includes fulfilling safeguarding duties, reporting to HMRC or the Charity Commission, maintaining financial records, and meeting other regulatory requirements relevant to charity governance and employment law.

4. Vital Interests

Actcessible does not routinely process personal data under the lawful basis of vital interests. However, this lawful basis may apply in exceptional circumstances, such as

where it is necessary to protect someone's life and the individual is physically or legally incapable of giving consent.

5. Public Task

Actcessible is not a public authority and does not undertake public tasks as defined under UK GDPR. Therefore, this basis is not applicable to the charity's data processing activities.

6. Legitimate Interests

Actcessible may process personal data under the lawful basis of legitimate interests, provided such processing is necessary, proportionate, and does not override the rights and freedoms of the data subject.

Examples of where this applies include processing personal data of trustees, volunteers, and freelance staff to:
• Communicate important information about the charity's meetings, activities, or training opportunities;
• Seek support, advice, or expertise where relevant to the individual's role or lived experience;
• Ensure individual access needs or adjustments are respected and planned for in meetings or events;
• Maintain accurate contact records to support safe, coordinated charity operations.

A legitimate interests assessment (LIA) will be carried out where appropriate to ensure that this basis is valid and justifiable.

Storing and Securing Data

We will take appropriate steps to store all data securely. This includes:

- Storing physical documents in locked cabinets
- Restricting digital access to authorised personnel only
- Protecting files with passwords and encryption where appropriate
- Not saving data to personal or unsecure devices
- Backing up data regularly and storing backups securely

Sensitive data (e.g., health information, ethnicity) will have heightened protections and will only be accessed on a strict need-to-know basis.

What is a Data Controller?

In the context of GDPR, a data controller for a UK charity is the organisation or entity that determines the purposes and means of processing personal data. Essentially, it's the charity

itself, or a specific part of it, that decides what personal data to collect, why it's needed, and how it will be used. This could be the charity's board of trustees, a specific department, or even an individual acting on the charity's behalf.

The data controller, carries the ultimate responsibility for ensuring that all processing of personal data complies with GDPR regulations. While Actcessible can delegate the actual processing of data to a third-party processor (like a mailing house for fundraising), the charity, as the controller, remains accountable for the overall compliance.

Actcessible is a data controller when it:

- Collects and uses personal data of donors for fundraising.
- Processes employee data for payroll and HR purposes.
- Handles data of volunteers for their involvement in the charity's activities.
- Provides services to beneficiaries and collects their personal information.

Data processor vs. data controller:

It's crucial to distinguish between a data controller and a data processor. A processor acts on behalf of the controller, carrying out specific tasks as instructed. While processors also have responsibilities under GDPR, the controller ultimately bears the responsibility for ensuring compliance.

What is a data processor?

In the context of GDPR, a data processor for a UK charity is an entity (like a company or individual) that processes personal data on behalf of the charity, which acts as the data controller. Essentially, the processor carries out tasks with the data according to the charity's instructions and for their purposes.

The data processor must ensure the security of the data they handle and process it according to the controller's instructions.

Who are Actcessible's data processors?

As Actcessible grows the data processors will almost certainly change. Currently the data processors are the Artistic Director, Robert Scott Henry, and the board of trustees. However, as the administrative burden grows the processors could include a volunteer administrator or a payroll processing firm or a marketing agency.

Who is the Data Controller for Actcessible?

The board of trustees is the data controller for Actcessible.

The board of trustees, as the data controller, will ensure that clear contracts will be in place between Actcessible and all external data processors, outlining how the data will be

processed and protected. It will also instruct and monitor the Artistic Director and, when applicable, all other internal data processors (whether employed or volunteer) to ensure the processing of data is in line with their autorisations.

What is a Third Party?

A third party is specifically defined as someone not the data subject (the individual whose data is being processed), the data controller (Actcessible - the entity determining how and why personal data is processed), or the data processor (the entity processing data on behalf of the controller).

Individuals or entities authorised by the controller or processor to process data under their direct authority are also not considered third parties. Examples could be a payroll company processing employee data on behalf of Actcessible, or an independent examiner checking that the accounts are in accordance with the underlying records, an IT support company maintaining Actcessible's computer system, a Cloud storage provider or Marketing agency. All these examples may process personal data, but do so on behalf of Actcessible (the data controller), not independently.

Data Sharing and Third Parties

We will not share personal data with third parties without a lawful basis. Where third parties process data on our behalf, we will:

- Ensure contracts include data protection clauses
- Conduct due diligence and security audits
- Confirm that data is not transferred outside the UK/EEA unless adequate safeguards are in place

Data Retention and Disposal

We will retain data only as long as necessary. Standard retention periods include:

- Staff and volunteer records: 6 years after role ends
- Participant data: 3 years after last activity
- Financial records: 7 years for accounting compliance

Data will be disposed of securely when no longer needed. This includes shredding paper and securely deleting digital files.

Individual Rights

Individuals have the right to:

- Be informed about the collection and use of their data
- Access the data we hold on them (Subject Access Request)
- Correct inaccurate or incomplete data

- Request erasure of their data in certain circumstances
- Object to processing based on legitimate interest or direct marketing
- Request the transfer of their data (data portability)

Requests must be submitted in writing and will be fulfilled within one calendar month, unless legally exempt.

Data Breaches

A data breach in the UK, under the UK GDPR, is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This can involve a wide range of situations, including data being lost, stolen, inappropriately accessed, altered without permission, damaged, or disclosed to unauthorised individuals.

The breach must involve personal data, which is information that can be used to identify an individual. Some examples of data breaches are:

- Loss or theft: Losing a laptop or paper files containing personal data.
- Cyberattacks: Ransomware attacks, hacking, or phishing attacks that compromise personal data.
- Human error: Sending an email to the wrong recipient, incorrectly processing data, or misplacing documents.
- Unauthorised access: Someone accessing data they are not authorised to view.

Any data breach must be reported to the DPL immediately. The DPL will:

Record the incident and assess its impact

- Take action to minimise harm
- Immediately notify the Information Commissioner's Office (ICO) if required, within 72 hours,
- In the event full details of the nature and consequences of the data breach are not immediately accessible the trustees will bring that to the affection of the ICO and undertake to forward the relevant information as soon as it becomes available.
- Inform affected individuals where there is a high risk to their rights and freedoms

Monitoring and Review

This document was adopted by the Actcessible Board of Trustees on: 28/07/2025

To be reviewed annually or as needed.

Signed (Trustee): 

Name: James Michael Dean

Date: 28/07/2025

Reviews will also be triggered by changes in legislation or significant incidents.

Data Protection Lead: David Owen (DPL) and Kyle Illsley (DDPL)

Email: [contact@actcessible.co.uk]

ICO Helpline: 0303 123 1113

Policy adopted by the Board of Trustees of Actcessible on [insert date].

Review due: [insert date].

To raise a data protection concern or make a Subject Access Request (SAR), email: contact@actcessible.co.uk