

**Data Protection Policy**

1. **Aims of this Policy**

**Upstart Scotland** needs to keep certain information on its employees, volunteers, and Trustees to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations. The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998 and the forthcoming General Data Protection Regulation. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this Policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

1. **Definitions**

In line with the Data Protection Act 1998 principles, **Upstart Scotland** will ensure that personal data will:

* 1. Be obtained fairly and lawfully and shall not be processed unless certain conditions are met;
	2. Be obtained for a specific and lawful purpose;
	3. Be adequate, relevant but not excessive;
	4. Be accurate and kept up to date;
	5. Not be held longer than necessary;
	6. Be processed in accordance with the rights of data subjects;
	7. Be subject to appropriate security measures;
	8. Not be transferred outside the European Economic Area (EEA).

The definition of ‘Processing’ is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper-based personal data as well as any kept on a computer.

The [Personal Data Guardianship Code](http://policy.bcs.org/sites/policy.bcs.org/files/Final%20copy.pdf) suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

1. Accountability: Those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
2. Visibility: Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
3. Consent: The collection and use of personal data must be fair and lawful and in accordance with the Data Protection Act’s [eight data protection principles](https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/). Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject’s consent should be explicitly obtained.
4. Access: Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
5. Stewardship: Those collecting personal data have a duty of care to protect this data throughout the data life span.
6. **Type of information processed**

**Upstart Scotland** processes the following personal information:

1. Members’ names, home & email addresses date of acceptance into membership by the Board of Trustees and date of cessation.
2. Personal information is kept in the following forms: in Microsoft Excel workbooks or similar and hard copies scanned as pdfs or stored as originals.
3. People within the organisation who will process personal information are: a Trustee appointed as the Data Controller overseen by the Chair and Secretary.
4. **Notification to the Information Commissioner**

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is David Ashford.

1. **Responsibilities**

Under the [Data Protection Guardianship Code](http://policy.bcs.org/sites/policy.bcs.org/files/Final%20copy.pdf), overall responsibility for personal data in a voluntary organisation rests with the governing body. In the case of **Upstart Scotland**, this is the Board of Trustees.

The governing body delegates tasks to the Data Controller. The Data Controller is responsible for:

* 1. understanding and communicating obligations under the Act;
	2. identifying potential problem areas or risks;
	3. producing clear and effective procedures;
	4. notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes.

All Trustees and volunteers who process personal information must ensure they not only understand but also act in line with this Policy and the data protection principles. Breach of this Policy will result in disciplinary proceedings.

1. **Policy Implementation**

To meet our responsibilities Trustees and volunteers will:

1. Ensure any personal data is collected in a fair and lawful way;
2. Explain why it is needed at the start;
3. Ensure that only the minimum amount of information needed is collected and used;
4. Ensure the information used is up-to-date and accurate;
5. Review the length of time information is held;
6. Ensure it is kept safely;
7. Ensure the rights people have in relation to their personal data can be exercised.

We shall ensure that:

1. Everyone managing and handling personal information is trained to do so;
2. Anyone wanting to make enquiries about handling personal information, whether a trustee, volunteer or member of staff knows what to do;
3. Any disclosure of personal data will be in line with our procedures;
4. Queries about handling personal information will be dealt with swiftly and politely.
5. **Gathering and checking information**

Before personal information is collected, we shall consider whether or not there is a need for it and if so, for how long.

We shall inform people whose information is gathered the reason for doing so and the extent of its use for the better execution of our purposes. Access to it will be restricted to the Data Controller and the Trustees.

We shall take measures to ensure that personal information is kept accurate and periodically refreshed by means of requesting the up-dating of it.

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

1. **Data Security**

**Upstart Scotland** will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

1. Any computer that contains the data will be kept safe and secure;
2. The password for access to the computer will be known only to the Data Controller and authorised Trustees;
3. When not in use, the computer and any related hard copies containing data will be kept under lock and key;
4. Any unauthorised disclosure of personal data to a third party may result in disciplinary proceedings or in the case of a Trustee’s breach of compliance with this Policy, personal liability for a penalty.
5. **Subject Access Requests**

Anyone whose personal information we process has the right to know:

* 1. What information we hold and process on her or him;
	2. How to gain access to this information;
	3. How to keep it up-to-date;
	4. What we are doing to comply with the Data Protection Act, the General Data Protection Regulation or any subsequent relevant legislation.

There is also the right to prevent processing of personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Data Protection Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to David Ashford, the Data Controller, via email namely: ashford37@btconnect.com. There may be a charge of £10 payable to **Upstart Scotland** on each occasion access is requested.

In any event, the following information will be required before access is granted:

* 1. full name and contact details of the person making the request;
	2. that person’s relationship with the organisation – e.g. former/current Member or volunteer;
	3. Any other relevant information reasonably required;
	4. Identification such as a passport, driving licence or birth certificate.

We shall aim to comply with requests for access to personal information as soon as practicable even though the Data Protection Act stipulates that must be done within forty days from receipt of written request and fee, if applicable.

1. **Review**

This Policy will be reviewed at intervals of three years to ensure it remains up-to-date and compliant with the law.

April 2018

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**