SP4 DATA PROTECTION POLICY

Policy Number	SP4
Policy Name	Data Protection Policy
Issue Date	September 2023
Review Date	September 2024
Owner	Data Protection Officer
Reviewing Body	Executive Team

Introduction

We are required to collect and use information about individuals with whom we deal in order to be able to operate effectively. These individuals include current, past and prospective employees, volunteers, people we support, funders, supporters and others with whom we communicate. The lawful and correct treatment of personal information is essential to building and maintaining the confidence with those with whom we have a relationship. The General Data Protection Regulation (GDPR), as supplemented by the Data Protection Act DPA
2018 (DPA), is the main piece of legislation that governs how we collect and process personal data.

1.0 Purpose

1.1 This policy describes how personal data must be collected, handled and stored to meet our data protection standards and to comply with the law.

1.2 This policy will benefit us by:

- promoting transparency and accountability;
- fostering a data protection culture across the Charity;
- ensuring compliance with the Regulations;
- ensuring employee confidence and compliance in their processing of personal data;
- reducing the risk of financial penalties and reputational damage;
- providing confidence to our community that personal data is being well managed;
- ensuring data subjects know how they can access their data.

2.0 Scope

2.1. This policy applies to all employees, permanent and temporary, contractors, volunteers and trustees. It applies to all personal data and special category personal data collected and processed by the Charity in the conduct of our business and includes both automated personal data and manual filing systems.

3.0 Duties and Responsibilities

3.1 The Board of Trustees

The Board of Trustees is ultimately responsible for ensuring that Autism Unlimited meets its legal obligations.

3.2 The Chief Executive

The Chief Executive has overall responsibility for the Charity's compliance with the regulations as a data controller and data processor.

3.3 Company Secretary

The Head of IT is the designated Data Protection Officer and is responsible for;

- Keeping the CEO and Trustees updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies in line with the agreed schedule;
- Maintaining the Charity's Data Protection notifications and reporting any necessary changes to the

- Office of the Information Commissioner;
- Arranging data protection training and advice;
- Handling data protection queries from anyone covered by this policy;
- Dealing with Subject Access Requests and coordinating the organisation's response;
- Advising on and approving Privacy Impact Assessments;
- Checking and approving contracts or agreements with third parties that may handle the Charity's
- sensitive data;
- Dealing with any queries from the Information Commissioner.

3.4 The Senior IT Technician is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party cloud applications the Charity is considering using to store or process data.

3.5 The Fundraising Manager is responsible for:

- Approving any data protection statements are attached to communications
- Coordinating any data protection queries from the media
- Ensuring fundraising and marketing initiatives abide by data protection principles
- Checking marketing databases against industry suppression files

3.6 The Operational Management Group (OMG)

The senior team in the Charity are responsible for:

- Promoting the need for data protection and the data protection policy;
- Ensuring that the policy is implemented, adhered to and monitored;
- Taking action to correct any weaknesses identified in implementation;
- Keeping up to date with best practice in their business area

3.7 All employees

All employees are responsible for:

- Every individual is responsible for ensuring that they meet the requirements of the Regulations, familiarising themselves with this policy and related documents;
- Completing the mandatory GDPR training courses

4.0 Related Documents

- Retention Guidelines
- Procedure for the management of Subject Access Requests
- Complaints policy

5.0 Data Protection Principles

The GDPR is based on a set of core principles that the Charity must observe and comply with at all times from the moment that personal data is collected to the moment that it is archived, deleted or destroyed. The Charity must ensure that all personal data is:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency)
- Collected only for specified, explicit and legitimate purposes (Purpose Limitation)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed (Data minimisation)
- Accurate and where necessary kept up to date (Accuracy)
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation)

- Processed in a manner that ensures its security by using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and or against accidental loss, destruction or damage (Security, integrity and confidentiality)

Additionally, we must ensure that:

- Personal data is not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA)or to another country without appropriate safeguards being in place (see Transfers of personal data outside of the EEA)
- Subjects can exercise their rights in relation to their personal data (see Data subject rights and requests)

5.1 Lawfulness, fairness and transparency

5.1.1 Lawfulness and fairness

In order to collect and process personal data for any specific purpose, the Charity must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, used or otherwise processed by the Charity. Processing personal data will only be lawful where at least one of the following lawful bases applies:

- The data subject has given their consent for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party
- (for instance a contract of employment);
- To comply with the Charity's legal obligations;
- To protect the vital interests of the data subject or another person;
- To perform tasks carried out in the public interest or the exercise of official duty.

5.1.2 Consent as a lawful basis for processing

There is no hierarchy between the lawful bases for processing data. In order for a data subject's consent to be valid and provide a lawful basis for processing, it must be:

- specific (not given in respect of multiple unrelated purposes);
- informed (explained in plain and accessible language) ;
- unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient);
- separate and unbundled from any other terms and conditions provided to the data subject ;
- freely and genuinely given.

The following principles must be observed;

- A Data Subject must be able to withdraw their consent as easily as they gave it.
- Once consent has been given, it will need to be updated where the Charity wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.
- Unless the Charity is able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained) will usually be required to process special categories of personal data.

5.1.3 Transparency

This requires the Charity to ensure that any information provided to Data Subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language

The Charity can demonstrate transparency through providing data subjects with appropriate privacy notices or fair processing notices before it collects and processes personal data and at appropriate times throughout the processing of personal data.

The GDPR sets out a detailed list of information that must be contained in all privacy notices and fair processing notices, including the types of personal data collected; the purposes for which they will be

processed; the lawful basis relied upon for such processing; the period for which they will be retained; and with whom the Charity may share the personal data.

5.2 Purpose limitation

The Charity must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects before the personal data has been collected.

The Charity must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where it intends to do so, it must inform the Data Subjects before using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

5.3 Data minimisation

The personal data that the Charity collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed. Personal data must only be processed when necessary for the performance of duties and tasks and not for any other purposes.

We may only collect personal data as required for the performance of our duties and tasks and should not ask a Data Subject to provide more personal data than is strictly necessary for the intended purposes.

We must ensure that when personal data is no longer needed for the specific purposes for which they were collected, such personal data are deleted, destroyed or anonymised.

5.4 Accuracy

The personal data that the Charity collects and processes must be accurate and, where necessary, kept up-to- date and must be corrected or deleted without delay when the Charity discovers, or is notified, that the data are inaccurate.
We must ensure that we update all relevant records if you become aware that any personal data is inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

5.5 Storage limitation

The personal data that the Charity collects and processes must not be kept in a form that identifies a data subject for longer than is necessary (except in order to comply with any legal, accounting or reporting requirements).

Storing personal data for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage. The Charity will maintain policies and procedures to ensure that personal data are deleted, destroyed or anonymised after a reasonable period of time following expiry of the purposes for which they were collected.

We must regularly review any personal data processed in the performance of our duties and tasks to assess whether the purposes for which the data was collected have expired. Where appropriate, we must take all reasonable steps to delete or destroy any personal data that is no longer required in accordance with Records Retention Schedule.

5.6 Security, integrity and confidentiality

5.6.1 Security of personal data
The personal data that the Charity collects and processes is secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

We are responsible for ensuring the security of the personal data processed in the performance of our duties and tasks. We must ensure that we follow all procedures in place to maintain the security of personal data from collection to destruction.

We must ensure that the confidentiality, integrity and availability of personal data are maintained at all times.

5.6.2 Data archives

Where data is archived either electronically or in paper form, the data should be clearly marked, referenced with the department and the data subjects to which it relates and entered onto the archiving log. The archiving log should record a reference for the archived data, a description of data archived, who is responsible for the data and when it can be disposed of.

5.6.3 Disposal of personal data

All materials containing personal information must be destroyed in a secure manner. Files and paper records should be shredded using the office shredders provided, placed in a secure, confidential paper bin or secured in a confidential waste bag for external destruction.

All personal information on Autism Unlimited computers and other electronic media must be completely removed before PCs, laptops, printers, photocopiers; scanners are disposed of or given to someone else.

6 .0 Data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All data breaches or suspected data breaches should be reported to the Data Protection Officer immediately.

All data breaches will be investigated and a formal report produced. The Data Protection Officer will consider the actions required and where appropriate will inform the Information Commissioner's office within 72 hours and any affected individuals without delay. A record of all data breaches is maintained by the Data Protection Officer.

7.0 Complaints

Autism Unlimited takes its responsibilities in relation to personal data seriously. All complaints will be dealt with in accordance with the complaints policy. This policy is available on request and is also available on the organisation's website.

8.0 Data subject rights and requests

The GDPR provides data subjects with a number of rights in relation to their personal data. These include:

- Right to withdraw consent: where the lawful basis relied upon by the Charity is the data subject's
- consent, the right to withdraw such consent at any time without having to explain why
- Right to be informed: the right to be provided with certain information about how we collect and
- process the data subject's personal data
- Right of subject access: the right to receive a copy of the personal data that we hold, including
- certain information about how the we have processed the data subject's personal data
- Right to rectification: the right to have inaccurate personal data corrected or incomplete dated completed
- Right to erasure (right to be forgotten): right to ask the that we delete or destroy the data subject's
- personal data if
- the personal data are no longer necessary in relation to the purposes for which they were collected;
- the data subject has withdrawn their consent (where relevant);
- the data subject has objected to the processing;
- the processing was unlawful;
- the personal data have to be deleted to comply with a legal obligation;
- the personal data were collected from a data subject under the age of 13, and they have
- reached the age of 13.
- Right to restrict processing: the right to ask the Charity to restrict processing if:

- the data subject believes the personal data is inaccurate;
- the processing was unlawful and the data subject prefers restriction of processing over
- erasure;
- the personal data is no longer necessary in relation to the purposes for which they were collected, but they are required to establish, exercise or defend a legal claim.
- Right to data portability: in limited circumstances, the right to receive or ask the Charity to transfer to a third party, a copy of the data subject's personal data in a structured, commonly used machine- readable format
- Right to object: the right to object to processing
- Right to object to direct marketing: the right to request that we do not process the data subject's
- personal data for marketing purposes
- Right to be notified of a personal data breach: the right to be notified of a personal data breach
- which is likely to result in a high risk to the data subject's rights or freedoms
- Right to complain: the right to make a complaint to the ICO or another appropriate supervisory authority

We must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. We must immediately forward any request made by a data subject (even if you are uncertain whether it represents a request as set out above) to the Data Protection Officer. The Charity will only have 30 days to respond in most circumstances. You must observe and comply with the Charity's data subject access requests procedure.

9.0 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for any new projects involving the use of personal data;
A DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks

6.0 Review

Annually