BeyondAutism

GDPR DATA PROTECTION POLICY

(Related policies: Data Retention; Privacy; Security Access; Subject Access Request; Access Control; Disciplinary)

Registered Charity in England and Wales No. 1082599. Registered Company No. 4041459.
Registered Office: Ashurst LLP, London Fruit & Wool Exchange, 1 Duval Square, London, E1 6PW

Contents

1. Introduction

This policy covers how information collected and processed by BeyondAutism relating to staff, governing bodies, volunteers, children and young adults, parents and supporters is gathered, used and stored. It should be used in conjunction with the related policies listed on the front.

It is important that all measures we have in place are designed to

- Meet our personal data obligations around how personal information is managed;
- Support our 5-year strategy and organisational objectives;
- Have appropriate systems and controls in place to reduce risk; and
- Safeguard personnel and stakeholder interests.

2. Policy statement

We recognise our responsibility under the General Data Protection Regulation (GDPR) and are committed to being compliant with all applicable UK and EU data protection legislation around the use of personal data as well as safeguarding the rights of the individuals whose information we collect. We will ensure that this Policy and all related policies are kept up to date and brought to the attention of all staff, including temporary staff, agency workers, contractors and volunteers working on behalf of the organisation.

All staff are expected to familiarise themselves with this policy. All new staff will be issued with a copy as part of the induction process. A copy is also available in the Staff Handbook.

3. Complying with the General Data Protection Regulation

Anyone processing personal data must comply with the enforceable principles of good practice contained within GDPR. This can be done by:

- Processing personal information only when it is absolutely necessary for organisational purposes;
- Ensuring that the least possible amount of personal data is collected, and that personal data is never processed unduly;
- Informing individuals of how their personal data is or will be used and by whom;
- Processing personal data in a lawful and fair manner;
- Keeping a record of the various categories of personal data processed;
- Ensuring that all personal data that is kept is accurate and up-to-date;

- Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes;
- Giving individuals the right of 'subject access', as well as all other individual rights around their personal data;
- Ensuring that all personal data is maintained securely;
- Transferring personal data outside of the EU only in situations where it is appropriately secured; and
- Identifying personnel that are responsible and accountable for GDPR Compliance.

We have registered with the Information Commissioner as a 'data controller' that engages in processing personal information of data subjects.

The Data Protection Officer ("DPO") will retain a copy of all notifications made by us to the Information Commissioner's Office ("ICO"). They are also responsible for each review of the GDPR Compliance, keeping in mind our activities. Data protection impact assessments will be used to ascertain any additional relevant requirements.

This policy applies to all employees of BeyondAutism. Breaches of the GDPR policy will be dealt with according to our **Disciplinary Policy**. If there is a possibility that the breach could amount to a criminal offence, the matter will be referred to the relevant authorities.

All third parties working with or for us who have, or may have, access to personal data are required to read, understand and fully comply with this policy at all times. They are required to enter into a data confidentiality agreement prior to accessing any personal data. We will at all times have the right to audit any personal data accessed by third parties, pursuant to the confidentiality agreement.

4. Definitions (as per the GDPR)

- Child means anyone under the age of 16.
- *Data controller* is a natural or legal person, or organisation, whether a public authority, agency or other body which, individually or jointly with others, is in charge of ascertaining the purposes and means by which personal data will be processed.
- *Data subject* refers to any living person who is the subject of personal data (see below for the definition of 'personal data') held by an organisation. A data subject is identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social.
- *Data subject consent* refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a written or oral statement or by clear, unambiguous action and must be given freely at all times, without duress, with the data subject being properly informed.
- *Personal data* means any information relating to a data subject.

- *Personal data breach* refers to a security breach which results in the disclosure, alteration, destruction or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully. All personal data breaches must be reported to the relevant regulatory authority by the 'data controller' at all times, whereas the data subject need only be informed of a data breach when it is likely that the breach will have an adverse effect on his or her privacy or personal data.
- *Processing* refers to any action taken in relation to personal data, including but not limited to collection, adaptation or alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise.
- *Special categories of personal data* refer to personal data covering such matters as racial or ethnic origin, beliefs – whether religious, political or philosophical, biometric identification, health, sexual orientation and sex life.
- *Third party* is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the controller or processor.

5. Responsibilities under the GDPR

We are a data controller and a data processor, under the definitions outlined by the GDPR.

Appointed employees with managerial or supervisory responsibilities are responsible for ensuring that good personal data handling practices are developed, reviewed and encouraged within the organisation, as per individual job descriptions.

Data Protection Officer

The position of DPO, which involves the management of personal data within BeyondAutism as well as compliance with the requirements of the DPA and demonstration of good practice protocol, is to be undertaken by iStorm

The DPO reports to the CEO and, amongst other things, is accountable for the development and day-to-day compliance with this policy, both in terms of security and risk management. In addition, the DPO is directly responsible for ensuring that we are GDPR compliant and that Heads of Services / Departments are compliant around the data processing that occurs within their field of responsibility and/or oversight.

The DPO is the first point of contact for any employees of BeyondAutism who require guidance in relation to any aspect of data protection compliance. They are also responsible for procedures such as Subject Access Requests.

You are all responsible for the personal data you process and should ensure your own compliance with data protection laws. Guidance on this can be found by reading this and the related policies. In addition, all employees, including volunteers and contract staff are required to read a document that makes you aware of the key elements of the GDPR which apply to our organisation and your role.

Risk Assessment

Risk assessments make us aware of the risks associated with the personal data processing we carry out. This also applies to the personal data processing undertaken by other organisations on our behalf. Identifying risks helps us mitigate the likelihood of potential non-compliance with this policy and with the GDPR.

Where personal data processing is carried out using new technologies, or when a high risk is identified in relation to the “rights and freedoms” of natural persons, we will carry out a risk assessment of the potential impact. More than one risk may be addressed in a single assessment (also known as a ‘Data Protection Impact Assessment’ (“DPIA”)).

If the outcome of a DPIA points to a high risk that our intended personal data processing could result in distress and/or may cause damage to data subjects, the DPO will then decide whether we ought to proceed and the matter should be escalated. In turn, the DPO may escalate the matter to the regulatory authority if significant concerns have been identified.

It is the role of the DPO to ensure that appropriate controls are in place to keep the risk level associated with personal data processing to an acceptable level, as per the requirements of the GDPR.

6. Principles of data protection

The principles of personal data processing are as follows:

1. All personal data must be processed lawfully and fairly at all times, as per our **Privacy Policy**.
2. Policies must be transparent, meaning that our personal data processing policies, as well as any specific information provided to a data subject, are readily available, easily accessible and clear, drafted using clear and plain language.
3. Data subjects must be provided with the following information, which can be found in our **Privacy Policy** or by contacting BeyondAutism:

- *Controller* – the identity and contact details of the data controller – in this case it is BeyondAutism;
- *DPO* – the contact details of the DPO;
- *Purpose* – the purpose or purposes and legal basis of processing;
- *Storage period* – the length of time for which we will store data;
- *Rights* – confirmation of the existence of the following rights:
    - Right to request access;
    - Right of rectification;
    - Right of erasure; and
    - Right to raise an objection to the processing of personal data;
- *Categories* – the categories of personal data;
- *Recipients* – the recipients and/or categories of recipients of personal data;
- *Location* – if we intend to make a transfer of personal data to a third country and the levels of data protection provided for by the laws of that country; and
- *Further information* – any further information required by the data subject to ensure that the processing is fair and lawful.

4. Personal data will only be collected for specified, explicit and legitimate reasons. When personal data is obtained for specific purposes, it will only be used in relation to that purpose.
5. Personal data must be adequate, relevant and restricted to only what is required for processing. The DPO will be involved in monitoring and providing advice, to:
    - Ensure that personal data which is superfluous and not necessarily required for the purpose(s) for which it is obtained, is not collected;
    - Check all new data collection form templates, whether in hard-copy or electronic format;
    - Carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant and not excessive; and
    - Securely delete or destroy any personal data that is collected in a manner that is excessive or unnecessary according to our GDPR policies.
6. Personal data must be accurate and up-to-date:
    - Data will not be kept unless it is reasonable to assume its accuracy and data that are kept for long periods of time will be examined and amended, if necessary;
    - All staff will receive training to ensure they fully understand the importance of collecting and maintaining accurate personal data;
    - Individuals are personally responsible for ensuring that the personal data held by us is accurate and up-to-date. We will assume that information submitted by individuals via data collection forms is accurate at the date of submission;
    - All employees of BeyondAutism are required to update the organisation as soon as reasonably possible of any changes to personal information, to ensure records are up-to-date at all times;
    - The DPO shall, on an annual basis, carry out a review of all personal data controlled by us; and

- The DPO will also ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are duly informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject involved. We will also provide an update to the third party, correcting any inaccuracies in the personal data.

7. The form in which the personal data is stored will be such that the data subject can only be identified when it is necessary to do so for processing purposes. The following principles apply:
   - Personal data that is kept beyond the processing date must be either encrypted or anonymised and kept to an absolute minimum, to ensure the protection of the data subject's identity should a data breach incident occur;
   - Personal data must be retained according to the **Data Retention Policy** and must be destroyed or deleted in a secure manner as soon as the retention date has passed; and
   - Should any personal data be required to be retained beyond the retention period set out in the **Data Retention Policy**, this may only be done after seeking advice from the DPO, which must be in line with data protection requirements.
8. The processing of personal data will always be carried out in a secure manner.
9. Personal data will not be processed in an unauthorised or unlawful manner, nor should it be accidentally lost or destroyed at any time and we will implement robust technical and organisational measures to ensure the safeguarding of personal data.

7. Security controls

Security controls are necessary to ensure that risks to personal data identified by us are appropriately mitigated as much as possible to reduce the potential for damage or distress to data subjects whose personal data is being processed and are subject to regular audit and review.

Personal data will not be transferred to a country outside of the EU unless the country provides appropriate protection of the data subject's 'rights and freedoms' in relation to the processing of personal data. This protection includes personal data that is held in cloud-based systems.

8. Accountability

According to the GDPR accountability principle, the data controller is responsible both for ensuring overall compliance with the GDPR and for demonstrating that each of its processes is compliant with the GDPR requirements. To this extent we are required to:

- Maintain all relevant documentation regarding our processes and operations;
- Implement proportionate security measures; and
- Carry out Data Processing Impact Assessments ("DPIAs");

9. The rights of data subjects

Data subjects enjoy the following rights in relation to personal data that is processed and recorded:

- The right to make access requests in respect of personal data that is held and disclosed;
- The right to refuse personal data processing, when to do so is likely to result in damage or distress;
- The right to refuse personal data processing, when it is for direct marketing purposes;
- The right to be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject;
- The right not to solely be subject to any automated decision-making process;
- The right to claim damages should they suffer any loss as a result of a breach of the provisions of the GDPR;
- The right to take appropriate action in respect of the following: the rectification, blocking and erasure of personal data, as well as the destruction of any inaccurate personal data;
- The right to request that the ICO carry out an assessment as to whether any of the provisions of the GDPR have been breached;
- The right to be provided with personal data in a format that is structured, commonly used and machine-readable;
- The right to request that his or her personal data is sent to another data controller; and
- The right to refuse automated profiling without prior approval.

10. Data access requests

Our **Subject Access Request Policy** sets out the procedure for making data access requests to data subjects and outlines how we will comply with the requirements of the GDPR on this.

11. Complaints

All complaints about our processing of personal data may be lodged by a data subject directly with the DPO by emailing **dpo@istormsoulutions.co.uk** providing details of the complaint. The data subject must be provided with a **Privacy Policy** at this stage.

If an individual is unhappy with the way their complaint has been handled or want to discuss any appeals following the submission of a complaint, they should contact the DPO.

12. Consent

Consent to the processing of personal data by the data subject must be:

- Freely given and should never be given under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information;
- Explicit;
- Specific;
- A clear and unambiguous indication of the wishes of the data subject;
- Informed;
- Provided either in a statement or by unambiguous affirmative action;
- Demonstrated by active communication between the data controller and the data subject and must never be inferred or implied by omission or a lack of response to communication; and
- In relation to sensitive data, consent may only be provided in writing, unless there is an alternative legitimate basis for the processing of personal data.

Employees

Usually, we will obtain consent to process personal and sensitive data when a new employee signs an employment contract or during induction programmes. Data subjects have the right to withdraw consent for non-operational functions at any time.

Other data subjects – Supporters, Volunteers or those engaging with our services

If using Consent as a condition to process data, we will obtain Consent in accordance with the procedures outlined in the policy framework. Consent is considered to be a positive action on behalf of the data subject having read a clear, transparent and unambiguous privacy notice. It does not necessarily have to be a box that is ticked, it could be the completion of a form, or the supply of contact information. We understand that according to

the Privacy and Electronic Communications Regulations (PECR) consent does not have to be explicit. We will use our judgement to decide how to obtain consent in different circumstances. However, we will always uphold the rights and freedoms of data subjects by always making it as easy to Opt-out as it ever was to Opt-in.

We mostly use Consent when promoting the aims and objectives of our organisation. We reserve the right to use it wherever we believe a data subject has indicated their wishes and where we have collected the data for that particular purpose. We only use data for the purpose for which it was collected.

13. Data security

All employees of BeyondAutism are personally responsible for keeping secure any personal data held by us for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless we have provided express authorisation and they have entered into a data processing agreement with us.

Accessing and storing personal data

Access to personal data is only granted to those who need it and only according to the principles of our **Security Access Policy**.

All personal data must be stored:

- In a locked room, the access to which is controlled; and/or
- In a locked cabinet, drawer or locker; and/or
- If in electronic format and stored on a computer, encrypted according to the corporate requirements set out in the **Security Access Policy**; and/or
- If in electronic format and stored on removable media, encrypted as per the **Security Access Policy**.

Before being granted access to any organisational data, all staff of BeyondAutism must understand and have a copy of the **Security Access Policy**.

Computer screens and terminals must not be visible to anyone other than staff with the requisite authorisation.

No manual records may be accessed by unauthorised employees of BeyondAutism and may not be removed from the business premises in the absence of explicit written authorisation. Manual records must be removed from secured archiving when access is no longer needed on a day-to-day basis.

All deletion of personal data must be carried out in accordance with our **Data Retention Policy**. Manual records which have passed their retention date must be shredded and any removable or portable computer media such as hard drives and USB sticks must be destroyed as per the **Security Access Policy** prior to disposal.

Personal data that is processed 'off-site' must be processed only by members of the Senior Management Team due to the increased risk of its loss, damage or theft.

14. Data access rights

Data subjects have the right to access all personal data in relation to them held by us, whether as manual records or electronic format. Data subjects therefore may at any time request to have sight of confidential personal references held by us as well as any personal data received by us from third-parties. To do so, a data subject must submit a **Subject Access Request**, as per the **Subject Access Request Policy**.

15. Disclosure of data

We take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the Police. All employees of BeyondAutism are required to access GDPR training in order to learn how to exercise due caution when requested to disclose personal data to a third party.

Disclosure is permitted by the GDPR without the consent of the data subject under certain circumstances, namely:

- In the interests of safeguarding national security;
- In the interests of crime prevention and detection which includes the apprehension and prosecution of offenders;
- In the interests of assessing or collecting a tax duty;
- In the interests of discharging various regulatory functions, including health and safety;
- In the interests of preventing serious harm occurring to a third party; and
- In the interests of protecting the vital interests of the data subject i.e. only in a life and death situation.

The DPO is responsible for advising on all requests for the provision of data for these reasons and authorisation by the DPO shall only be granted with support of appropriate documentation.

16. Data retention and disposal

We will not retain personal data for longer than is necessary and once an employee has left, it may no longer be necessary for us to retain all the personal data held in relation to that individual. Where personal data needs to be disposed of, this will be in line with our disposal procedures in our **Security Access Policy**. Some data will need to be kept longer than others, in line with our **Data Retention Policy**.

17. Review and Revision

This policy is to be periodically reviewed according to the requirements stipulated herein. The latest version of this document is available to all employees on Level 1 of the BeyondAutism Server.

Last review: October 2023

Review group: Trustees

Date of next review: October 2026

Registered Charity in England and Wales No. 1082599. Registered Company No. 4041459.
Registered Office: Ashurst LLP, London Fruit & Wool Exchange, 1 Duval Square, London, E1 6PW