BEYOND LIMITS

Beyond the limits of conventional support

DATA PROTECTION POLICY

This policy aims to provide important direction and guidance on how we process personal data and share information that applies to all staff.

Review: May 2027

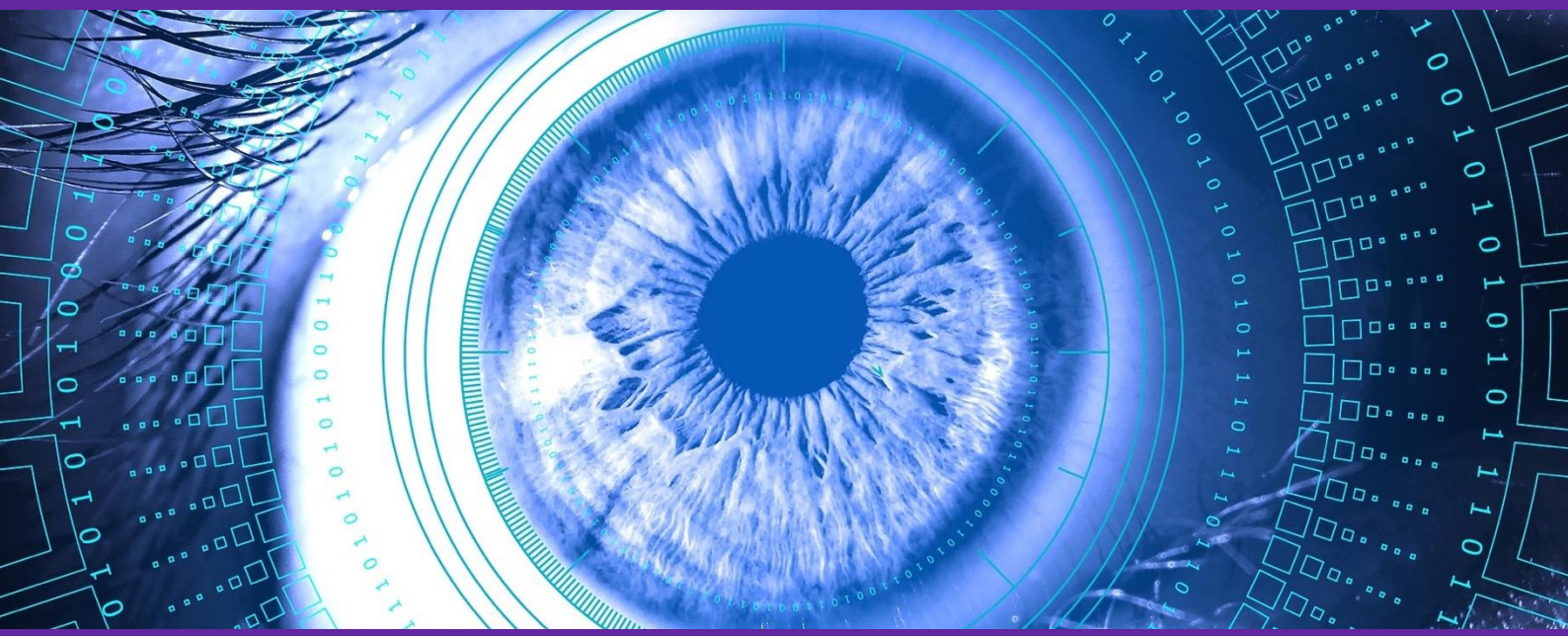
BEYOND LIMITS
Beyond the limits of conventional support

PURPOSE

This Data Protection policy aims to provide important direction and guidance on how we process personal data and share information that applies to all staff.

Our approach to Data Protection is defined by the conditions of the General Data Protection Regulation (GDPR), applied from 25th May 2018.

CONTENTS



SECTION ONE: INTRODUCTION

Beyond Limits collects and uses personal information ("personal data") about individuals accessing our support, as well as colleagues and other relevant individuals as required. This information is gathered as is consistent with our duty as a responsible provider of support for vulnerable individuals living in the community. In addition, we may be required by law to collect, use, and share certain information on a case-by-case basis.

The General Data Protection Regulation ("the Regulation") regulates the processing of personal data.

It protects the rights and privacy of all living individuals, which means protecting their personal data. For example, personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images, etc.), and may include facts or opinions about a person. All individuals who are the subject of personal data gathering have a general right of access to the personal data that relates to them.

THE REASON FOR THIS POLICY

- **People have legal rights with regard to the way their personal data is handled.**
- **In the course of our business activities we collect, store (i.e., retain) and process personal data about individuals accessing our support services, as well as colleagues and other third parties. Therefore, in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data.**
- **All people working in or with our business are obliged to comply with this policy when processing personal data.**

ABOUT THIS POLICY

- This policy sets out the basis upon which we will process personal data we collect from data subjects. For example, individuals accessing support and business contacts, or that which is provided to us by data subjects or other sources.
- It also sets out our obligations in relation to data protection under the General Data Protection Regulation ("GDPR").
- This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer, and store personal data.
- The procedures and principles set out herein must be followed at all times by all colleagues, agents, contractors, or other parties working on behalf of Beyond Limits.
- We aim to ensure the correct, lawful, and fair handling of personal data and to respect legal rights.

SECTION TWO: INFORMATION SHARING (IN THE CONTEXT OF SAFEGUARDING)

Beyond Limits provide support to individuals with learning difficulties, mental health illness and other support needs.

As a Data Controller, Beyond Limits holds highly sensitive personal data about those individuals, as well as colleagues and contractors. This is essential to our business as a responsible provider, but moreover it is a critical part of keeping individuals from harm or abuse.

The personal data we use is processed in accordance with strict conditions of confidentiality. These conditions must be maintained at all times and colleagues are bound by a clearly defined confidentiality agreement.

Beyond Limits fully recognise that there are occasions where sensitive information must be shared with relevant authorities, and professionals. For example:

- Effective sharing of information between practitioners and local agencies is essential for early identification of need, assessment, and service provision.
- Sharing information increases our capacity to take action to keep individuals safe from harm, as well as the wider community.
- Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare of individuals.
- Information may be shared without consent if a practitioner judges that there is good reason to do so, and that the sharing of information will enhance the safeguarding of the individual in a timely manner. When decisions are made to share information, practitioners must record who has been given the information, and why.

SECTION THREE: THE MEANING OF KEY DATA PROTECTION TERMS

KEY TERMS & THEIR MEANING:

- **DATA** is information that is stored electronically, on a computer, or in certain paper-based filing systems.
- **DATA SUBJECTS** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
- **PERSONAL DATA** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name or date of birth) or it can be an opinion about that person (i.e., actions and behaviours).
- **DATA CONTROLLERS** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the GDPR. We are the data controller of all personal data used in our business for our own commercial purposes.
- **PROCESSING** is any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to third parties.

SECTION FOUR: SUMMARY OF DATA PROTECTION PRINCIPLES

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply.

This means that all personal data must be subject to:

- **(LAWFULNESS, FAIRNESS AND TRANSPARENCY)** processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **(PURPOSE LIMITATIONS)** 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.

All data must be processed in line with data subjects' rights, in particular the right to:

1) Request access to any data held about them by a Data Controller.
2) Prevent the processing of their data for direct-marketing purposes.
3) Ask to have inaccurate data amended.
4) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

- (DATA MINIMISATION) adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- (ACCURATE) accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased, or rectified without delay.
- (STORAGE LIMITATIONS) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 Regulation in order to safeguard the rights and freedoms of the data subject.
- (INTEGRITY AND CONFIDENTIALITY) data safeguarding – 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.

Transfers outside UK must not be transferred to people or organisations situated in countries without adequate protection.

SECTION FIVE: DATA PROTECTION STATEMENT

We collect, hold, and process personal data for the purpose of maintaining high quality support to individuals with learning difficulties and/or mental health illness.

The following personal data may be collected, held, and processed by Beyond Limits:

Beyond Limits collects and uses personal information ("personal data") about individuals accessing support, as well as other relevant individuals as required. We may be required by law to collect, use, and share certain information. This is always on a case-by-case basis and the data subject's rights remain at the forefront of our approach.

SECTION SIX: OUR SPECIFIC DATA PROTECTION MEASURES

When working with personal data, we take the following measures:

- All emails containing personal data must be encrypted. Our email provider holds ISO/IEC 27001:2013.

  This is a standard for creating an Information Security Management System (ISMS). ISO 27001 is recognised as the "cornerstone" for any organisation that is "serious about combatting threats to information security, including cybercrime."

- Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded; An entry should be made in the destruction register (Note: A destruction register should be available in the staff office). Electronic copies should be deleted securely. This means:

  a) (For Mac Users) select "Secure Empty Trash;"
  b) (For Windows Users) Use a third-party wiping program, like 'CCleaner' or 'Eraser' (Eraser can also cleanse unallocated disk space).

- Personal data may be transmitted over secure networks only. Transmission over unsecured networks is not permitted in any circumstances and may result in disciplinary measures.
- Personal data should not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
- Where Personal data is to be sent by facsimile, transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or send using First Class Recorded Special Delivery and marked as 'Confidential.'
- No personal data may be shared informally and if a member of staff, agent, sub-contractor, or other party working on behalf of Beyond Limits requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer ("DPO"). The Data Protection Officer is Jill Barbour.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar.

- No personal data may be transferred to any colleagues, agents, contractors, or other parties,
- whether such parties are working on behalf of Beyond Limits or not, without the authorisation of the DPO. Note: The nature of Beyond Limits' business means that individual case files must be shared with relevant colleagues to ensure that there is sufficient and appropriate knowledge of the individual's needs and presentation.
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time.
- Personal data must not be included in telephone messages. If you need to speak to someone about an individual, please request a callback.
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise [without the formal written approval of the DPO and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary. Please note: Colleagues with access to company mobile telephones must ensure that files are deleted in a timely way.
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Beyond Limits where the party in question has agreed to comply fully with the letter and spirit of this policy and GDPR (which may include demonstrating to Beyond Limits that all suitable technical and organisational measures have been taken).
- All personal data stored electronically should be backed up no less than once a week. All backups should be encrypted and secure.
- All electronic copies of personal data must be stored securely.
- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. Where in place, colleagues must use multi-step authentication processes. Passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by Beyond Limits is designed to require such passwords.
- Under no circumstances should any passwords be written down or shared between any colleagues, agents, contractors, or other parties working on behalf of Beyond Limits, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.
- Personal data is not used by Beyond Limits for marketing purposes, without the explicit

authority of the data subject.

SUMMARY OF DATA PROTECTION MEASURES

Beyond Limits aim to ensure that colleagues have suitable and robust information security measures in place. Colleagues have a duty to inform the DPO if there are any concerns about the security measures. In addition, colleagues must:

- Not use sub-processors without DPO consent, who will require full details of rationale and purpose.
- Co-operate with the relevant Data Protection Authorities in the event of an enquiry.
- Report data breaches to the DPO without delay – within 72 hours.
- Keep records of all processing activities.
- Comply with EU trans-border data transfer rules.
- Maintain confidentiality regarding data subject's rights.
- Assist management in managing the consequences of data breaches.
- Not view CCTV recordings without the express permission of the data controller.
- Ensure that CCTV is only used for the purposes of detecting criminality.
- Ensure that CCTV recordings are held for no longer than 31 days, subject to any Police requirements following an incident. Retention times may vary depending upon the severity of the incident monitored.
- Delete or return all personal data at the request of management.
- Inform the DPO if the processing instructions potentially infringe GDPR compliance.

SECTION SEVEN: DATA PROTECTION PRINCIPLES

ONE: LAWFULNESS, FAIRNESS & TRANSPARENCY

The GDPR is not intended to prevent the processing of personal data. However, it does aim to ensure that the processing of personal data is done fairly and without adversely affecting the rights of the data subject. The processing of personal data is lawful, if one (or more) of the following applies:

- **(CONSENT)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- **(CONTRACT)** processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
- **(LEGAL OBLIGATION)** processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

- **(PROTECTION) processing is necessary to protect the vital interests of the data subject or of**
- **another natural person.**
- **(PUBLIC INTEREST) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.**
- **(LEGITIMATE INTERESTS) processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child aged less than 18 chronological years.**

TWO: PURPOSE LIMITATIONS

Beyond Limits collects and processes the personal data set out in Section Five of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and can include data received from third parties.

Beyond Limits only processes personal data for the specific purposes set out in Section Four of this policy (or for other purposes expressly permitted by the GDPR).

The purposes for which Beyond Limits process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

THREE: DATA MINIMISATION

Beyond Limits will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Section Five, above.

FOUR: ACCURATE

Beyond Limits shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter.

In addition, managers are responsible for checking the continued accuracy of data. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

FIVE: STORAGE LIMITATIONS

Beyond Limits shall not keep personal data for any longer than is necessary. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

SIX: SECURE PROCESSING

Beyond Limits shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. There will be:

- **An assessment of the risks posed to individual data subjects.**
- **Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the GDPR.**

SECTION EIGHT: DATA PROTECTION RIGHTS

The GDPR sets out the following rights applicable to data subjects:

- **The right to be informed.**
- **The right of access.**
- **The right to rectification.**
- **The right to erasure (also known as the 'right to be forgotten').**
- **The right to restrict processing.**
- **The right to data portability.**
- **The right to object.**
- **Rights with respect to automated decision-making and profiling.**

KEEPING DATA SUBJECTS INFORMED

Beyond Limits seek to ensure that the following information is provided to every data subject when personal data is collected:

- **Details of Beyond Limits ("the Company") including, but not limited to, the identity of Jill Barbour its Data Protection Officer (DPO).**
- **The purpose(s) for which the personal data is being collected and will be processed (as detailed in Section Four of this Policy) and the legal basis justifying that collection and processing.**
- **Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data.**

- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.
- Where the personal data is to be transferred to one or more third parties, details of those parties.
- Where the personal data is to be transferred to a third party that is located outside of the United Kingdom (the "UK"), details of that transfer, including but not limited to the safeguards in place.
- Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined).
- Details of the data subject's rights under the GDPR.
- Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time.
- Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the GDPR).
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection/processing of the personal data and details of any consequences of failing to provide it.
- Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.
- The information set out above shall be provided to the data subject at the following applicable time:

a) Where the personal data is obtained from the data subject directly, at the time of collection.
b) Where the personal data is not obtained from the data subject directly (i.e., from another party).
c) If the personal data is used to communicate with the data subject, at the time of the first communication, or
d) If the personal data is to be disclosed to another party, before the personal data is disclosed, or
e) In any event, not more than one month after the time at which the Company obtains the personal data.

SECTION NINE: SUBJECT ACCESS REQUESTS (SAR)

A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them.

Beyond Limits will usually respond to SARs within one month of receipt of the request. This can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

All subject access requests received must be forwarded to Jill Barbour, the Beyond Limits DPO. Jill may be contacted using the following details:

Email: Jill.Barbour@beyondlimits-uk.org
Phone: 01752 546449
Address: Unit 4 Stoke Damerel Business Centre, Church Street, Plymouth, Devon, PL3 4DT.
ICO Registration Number: Z336444X

Beyond Limits do not charge a fee for the handling of normal SARs. However, we reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

ALL DATA SUBJECTS HAVE A RIGHT OF ACCESS TO THEIR OWN PERSONAL DATA.

To ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Where a request for subject access is received from an individual accessing support, we expect that:

- **Requests from individuals accessing support will be processed as any subject access request. This is outlined below (SECTION TEN), and the copy will be given directly to the individual, unless it is clear that they do not understand the nature of the request or there are legal conditions prohibiting such action.**
- **Requests from individuals who do not appear to understand the nature of the request will be referred to those with suitable responsibility.**
- **All requests will be duly processed subject to any restrictive legal conditions.**

SECTION TEN: HANDLING SUBJECT ACCESS REQUESTS (SAR)

Requests must be made in writing using a Subject Access Request (SAR) form. Provided there is sufficient information to process the request, colleagues must record:

- **The date of receipt of request.**
- **The data subject's name.**
- **The name and address of requester.**
- **The type of data required.**

- **The planned date of supplying the information (normally not more than 40 days from the request date), should the request be considered appropriate.**

PLEASE NOTE: Should more information be required to establish the identity of the data subject or the type of data requested, the date in the log will be date upon which information has been provided.

SECTION ELEVEN: DATA RECTIFICATION OF PERSONAL DATA

If a data subject informs Beyond Limits that personal data held by the company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be reviewed and rectified as appropriate, with a clear focus upon accuracy.

The data subject will be informed of that rectification within one month of receipt the data subject's notice. (N.B. this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

In addition, a notification may be sent to the Information Commissioner's Office (ICO), with whom Beyond Limits are registered. This will be decided upon a case-by-case basis, ensuring that the threshold or notification is met. The threshold is based upon risk to people. This means whether or not people's rights and freedoms have been compromised following the breach.

The ICO are clear that we do not need to report every breach. If in any doubt, colleagues and other relevant stakeholders should speak with the DPO.

SECTION TWELVE: ERASURE OF PERSONAL DATA

Data subjects may request that Beyond Limits erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for Beyond Limits to hold that personal data with respect to the purpose for which it was originally collected or processed.
- The data subject wishes to withdraw their consent to Beyond Limits holding and processing their personal data, depending upon any legal conditions regarding the

individual and compliance regarding case file retention.

- The data subject objects to Beyond Limits holding and processing their personal data (and there is no overriding legitimate interest to allow Beyond Limits to continue doing so).
- The personal data has been processed unlawfully.
- The personal data needs to be erased in order for Beyond Limits to comply with a particular legal obligation.

Unless Beyond Limits have reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with. The data subject informed of the erasure, within one month of receipt of the data subject's request. (N.B. This can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

SECTION THIRTEEN: RESTRICTION OF PERSONAL DATA PROCESSING

Data subjects may request that Beyond Limits ceases processing the personal data it holds about them.

If a data subject makes such a request, Beyond Limits shall retain only the amount of personal data pertaining to that data subject that is necessary (in accordance with our legal obligations to hold and share certain information) to ensure that no further processing of their personal data takes place.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

SECTION FOURTEEN: DATA PORTABILITY

All relevant stakeholders should be aware that:

- Beyond Limits do not use *automated individual* decision-making software.
- Beyond Limits do not use personal data for automated individual decision-making (i.e., making a decision solely by automated means without any human involvement)

- **Beyond Limits does not use automated personal data profiling (i.e., automated processing of personal data to evaluate certain things about an individual).**

The personal data of individuals and, in exceptional circumstances, colleagues will only be sent to another Data Controller with an implicit legal basis that can be described as a "legitimate need." For example,

personal data relating to placement planning information and risk assessments, needs analysis well other matters relating to operating a responsible business.

SECTION FIFTEEN: OBJECTIONS TO DATA PROCESSING

Data subjects have the right to object to Beyond Limits processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to Beyond Limits processing their personal data based on its legitimate interests, Beyond Limits shall cease such processing forthwith, unless it can be demonstrated that Beyond Limits' legitimate grounds for such processing override the data subject's interests, rights, and freedoms; or the processing is necessary for the conduct of legal claims.

If a data subject objects to Beyond Limits processing their personal data for direct marketing purposes, Beyond Limits shall cease such processing forthwith.

Where a data subject objects to Beyond Limits processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'.

Please note that Beyond Limits is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

SECTION SIXTEEN: AUTOMATED DECISION-MAKING

Beyond Limits does not use *automated individual* decision-making software.

SECTION SEVENTEEN: PROFILING

Where Beyond Limits uses personal data for profiling purposes, the following shall apply:

- Clear information explaining any profiling will be provided, including its significance and the likely consequences.
- Appropriate mathematical or statistical procedures will be used.
- Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented.
- All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

Beyond Limits is clear that profiling will only be used for the following:

- Strategic development, specifically regarding regular analysis of the needs of individuals accessing support and commissioning authorities. This will be an internal process, and any data generated will be anonymised and maintained within the organisation.
- Matching and impact assessments of placement referrals, specifically profiling the safety and presentation needs of those accommodated against those referred.

Beyond Limits is clear that profiling will not be used for the following:

- Marketing (including advertising and publicity materials).

To comply with the GDPR, Beyond Limits:

- Have a lawful basis to carry out profiling (that is documented in this policy).
- Only collect a minimum amount of data needed and have a clear retention policy (that is documented in this policy).

SECTION EIGHTEEN: ACCOUNTABILITY

Beyond Limits Data Protection Officer (DPO) is Jill Barbour. Jill may be contacted using the following details:

Email: jill.barbour@beyondlimits-uk.org
Phone: 01752 546449
Address: Unit 4 Stoke Damerel Business Centre, Church Street, Plymouth, Devon, PL3 4DT.

ACCOUNTABILITY STATEMENT

Beyond Limits shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of Beyond Limits, its DPO, and any applicable third-party Data Controllers.
- The purposes for which Beyond Limits processes personal data.
- Details of the categories of personal data collected, held, and processed by Beyond Limits, and the categories of data subject to which that personal data relates.
- Details (and categories) of any third parties that will receive personal data from Beyond Limits.
- Details of any transfers of personal data to non-EEA countries (inc. all security safeguards).
- Details of how long personal data will be retained by Beyond Limits.
- Detailed descriptions of all technical and organisational measures taken by Beyond Limits to ensure the security of personal data.

SECTION NINETEEN: PRIVACY IMPACT ASSESSMENTS

Beyond Limits shall carry out Privacy Impact Assessments (PIA) as required under the GDPR. Privacy Impact Assessments shall be overseen by **Beyond Limits'** DPO and shall address the following:

- The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data.
- Details of the legitimate interests being pursued by Beyond Limits.
- An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.

SECTION TWENTY: OPERATIONAL MEASURES

Beyond Limits shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All colleagues, agents, contractors, or other parties working on behalf of Beyond Limits shall be made fully aware of both their individual responsibilities and Beyond Limits' responsibilities under the GDPR and under this policy and shall be provided with a copy of this policy.
- Only colleagues, agents, sub-contractors, or other parties working on behalf of Beyond Limits that need access to, and use of, personal data in order to carry out their assigned duties

- correctly shall have access to personal data held by Beyond Limits.
- All colleagues, agents, contractors, or other parties working on behalf of Beyond Limits handling personal data will be appropriately trained to do so.
- All colleagues, agents, contractors, or other parties working on behalf of Beyond Limits handling personal data will be appropriately supervised.
- Methods of collecting, holding, and processing personal data shall be regularly reviewed.
- The use of non-authorised (off the shelf) generative A.I. is not permitted.
- The performance of those employees, agents, contractors, or other parties working on behalf of Beyond Limits handling personal data shall be regularly evaluated and reviewed.
- All colleagues, agents, contractors, or other parties working on behalf of Beyond Limits handling personal data will be bound to do so in accordance with the GDPR and this policy.
- All agents, contractors, or other parties working on behalf of Beyond Limits handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as defined by this policy and the GDPR.
- Where any agent, contractor or other party working on behalf of Beyond Limits handling personal data fails in their obligations under this policy that party shall indemnify and hold harmless Beyond Limits against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

SECTION TWENTY-ONE: TRANSFERRING PERSONAL DATA OUTSIDE THE EEA

The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

CLARIFICATION OF THE EUROPEAN ECONOMIC AREA (EEA)

EU states which form part of the EEA

EFTA states which form part of the EEA

EU state which forms part of the EEA through the provisional application of an accession agreement

EFTA state which signed the EEA agreement but did not join

You may only transfer Personal Data outside the EEA if <u>one</u> of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms.

- Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO.

- The Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks.

- The transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

SECTION TWENTY-TWO: DATA BREACH NOTIFICATIONS

ALL PERSONAL DATA BREACHES MUST BE REPORTED IMMEDIATELY TO THE DPO.

If a personal data breach is identified and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g., financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPO must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours.

In the event that a personal data breach is likely to result in a high risk (to the rights and freedoms of data subjects), the DPO must ensure that all affected data subjects are informed of the breach directly and without delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO (or other contact point where more information can be obtained)

- **The likely consequences of the breach.**
- **Details of the measures taken, or proposed to be taken, by Beyond Limits to address the breach including, where appropriate, measures to mitigate its possible adverse effects.**