BEYOND LIMITS

Policies and Procedures

Beyond Limits provides policies and procedures to promote safe and consistent practice across the Organisation. The framework laid down within our policies and procedures lets everyone know how we work and reflects our values and mission statement. Our policies and procedures are written to help us, employees of Beyond Limits, to make good, safe decisions.

Beyond Limits expects all employees to be familiar with the contents of all policies and procedures relevant to their role and to understand how to apply them within their daily work.

None of these documents stand alone, all fit within the larger framework of the way we work and any associated policies which are particularly relevant will be directly referenced.

Data Protection Policy

Data Protection Policy – what this means to Beyond Limits

Beyond Limits recognises its statutory duty to comply with all relevant legislation and the duties and obligations resulting from them. The purpose of this Data Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the General Data Protection Regulation (2016) and the Data Protection Act (2018)

This should be read in conjunction with our relevant policies: Computer Use, Confidentiality, Information, Security and Networks Security and Duty of Candour.

We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

Beyond Limits is committed to the protection of its employees and others, including members of the public, from harm or loss resulting the activities and undertakings of Beyond Limits. Adequate resources will be made available to ensure the success of this policy.

The purpose of this policy is to enable Beyond Limits to:

- Comply with the law in respect of the data it holds about individuals
- Follow good practice

- Protect the "rights and freedoms" of our stakeholders and any other individuals whose information Beyond Limits collects and processes in accordance with the General Data Protection Regulation (GDPR)
- Protect the organisation from the consequences of a breach of its responsibilities

Beyond Limits will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff and volunteers who handle personal data, so they can act confidently and consistently

Beyond Limits recognises that its first priority under the GDPR is to avoid causing harm to individuals. In the main this means that personal data must be:

- Kept securely in the right hands
- Processed lawfully, fairly and transparently
- Collected for specific, explicit and legitimate purposes
- Adequate and kept up to date with every effort to erase or rectify without delay
- Kept in a form such that the data subject can be identified only as long as is necessary for processing
- Processed in a manner that ensures the appropriate security

Beyond Limits has identified the following potential risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately)
- Insufficient clarity about the range of uses to which data will be held – leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access
- Harm to individuals if personal data is not up to date

Due to our size, we have determined that we are not required to have a Data Protection Officer (DPO), as we do not process special categories of data on a large scale. Nonetheless, to ensure that every person's data rights are respected and that there is the highest levels of data security and protection in our organisation, we have appointed a member of staff to the Data Protection Lead (DPL) who reports

to the Director of Beyond Limits. We support the DPL with the necessary resources to carry out their tasks and ensure that they can maintain expertise. The Data Protection Lead is currently Jill Barbour, with the following responsibilities:

- Keeping up to date with ICO guidance
- Reviewing GDPR training and related policies
- Advising other staff on GDPR issues
- Handling notifications and subject access requests
- Reviewing the Business Continuity Plan procedures for security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of Beyond Limits
- Register with the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT
- Advising the Director of unusual or controversial disclosures of personal data

During their induction week all staff are required to take part in mandatory data protection training and read, understand and accept any policies and procedures that relate the personal data that they handle during their work. These include the General Data Protection Regulation Policy, Employee Handbook, Clean Desk Policy, Computers/Information Technology (including Mobile Phones and & Social Networking) Policy and Confidentiality Policy. These policies are available on the staff area of our website. Any volunteer staff would be inducted as our employees during an induction course.

Significant breaches of this policy will be handled under Beyond Limits disciplinary procedures.

Data Collection

Beyond Limits will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person or by completing a form.

When collecting data from employees and the people we support, Beyond Limits will ensure that the person:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are, should the person decide not to give consent to processing
- Grants explicit consent of the intended processing, either written or verbal for data to be processed. Consent cannot be inferred from non-response to a communication
- Is, as far as reasonably practicable, competent to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

- The data subject can withdraw their consent at any time

Data Storage and Retention

Information and records relating to people supported, staff, students, volunteers or any other relevant person will be stored securely and will only be accessible to authorised personnel.
Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. Beyond Limits aims to ensure personal data is disposed of when no longer needed to reduce the risk that it will become inaccurate, out of date or irrelevant.

Beyond Limits also wish to make reductions in the use of paper that is used in the business and the filing space we need. On an annual basis we review the information and records held by Beyond Limits and will assess whether to securely destroy (by shredding or deleting) or to electronically archive any such records held. Any archived data will also be reviewed annually.

During this procedure the Data Protection Lead should:

- Review the length of time we keep personal data
- Consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it goes out of date

It is the responsibility of Beyond Limits to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed/sold to a third party.

> **The home of the person you support is not an office, therefore the minimum amount of organisational records should be stored in the persons house.**

Ownership and Access to Records

Access to records is governed by the GDPR 2016 and has to respect the rules of confidentiality. Beyond Limits must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Beyond Limits' business. All requests to provide data for one of these reasons **must be** authorised by a Director.

Records kept by employees of Beyond Limits are owned by Beyond Limits and should only be shared on a "need to know" basis. Good practice means that records kept about a person being supported should be accessible to them. The only time rules on confidentiality in record-keeping can be over-ridden is in situations of public or personal safety or in relation to adult or child safeguarding.

Handling of Subject Access Requests

Beyond Limits recognises the rights of individuals who want to see a copy of the information the organisation holds about them and will process "subject access requests" in a co-operative and timely manner. Any such request will be dealt with promptly in line with GDPR 2016 and guidelines published on the Information Commissioner's Office website (https://ico.org.uk/for- organisations/guide-to-data-protection/principle-6-rights/subject-access-request/) and a fee will not usually be charged. We may however charge a reasonable fee if your request for access is clearly unfounded or excessive.

Freedom of Information Requests

Beyond Limits will assist and co-operate with its commissioning authorities to enable them to comply with their obligations under the Freedom of Information Act 2000. In all cases, the Data Protection Lead will be the point of contact for leading this process.

Sharing Information with the Commissioners and other Authorised Partners

During our ordinary course of business, Beyond Limits employees may be required to share information with commissioners and other authorised partners on a regular basis. Sharing sensitive personal data should only be undertaken electronically and when authorised to do so, using their Beyond Limits encrypted Egress email account or NHS Email Account. Personal details should be kept to a minimum and initials should be used rather than the name of anyone we support.

Data Access and Accuracy

All individuals have the right to access the information Beyond Limits holds about them. Beyond Limits will take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, Beyond Limits will ensure that:

- It has a Data Protection Lead with specific responsibility for ensuring compliance with GDPR
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately supervised and trained to do so
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It will regularly review and audit the ways it holds, manages and uses personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR 2016.

In case of any queries or questions in relation to this policy, please contact the Data Protection Lead for Beyond Limits: Jill Barbour, 01752 546449.

Employee Privacy Statement

Scope

Beyond Limits is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR). It applies to all employees, workers and contractors

Responsibilities

Beyond Limits is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Privacy notice

Our Data Protection Lead can be contacted directly here:

- jill.barbour@beyondlimits-uk.org
- 01752 546449

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

Your Personal Data

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status.
- Next of kin and emergency contact information.
- National Insurance number, Bank account details, payroll and pension records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date, Location of employment or workplace.
- Copy of driving licence and car insurance details.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Performance information.

- Disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Photographs.
- Support & Supervision, Annual Appraisal and Personal Development Plans.

Special Categories

There are "special categories" of more sensitive personal data which require a higher level of protection. We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information collected through our Equal Opportunities Monitoring Form about your age, marital status, ethnic origin, disability, gender and where you saw our advertisement.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

Collection of Data

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies. For your information, these are detailed on page 13 of this policy.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered in to with you.
- Where we need to comply with a legal obligation.

- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations which are likely to be rare:

- Where we need to protect your interests or someone else's interests
- Where it is needed in the public interest or for official purposes

Use of your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.

- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of Purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Sensitive Personal Information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

We will use your particularly sensitive personal information in the following ways:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations and in line with our Data Protection Policy.

3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme and in line with our Data Protection Policy.

4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about employee/workers/contractors or former employees/workers/contractors in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Consent

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data.

If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our Data Protection Policy.

Less commonly, we may use general information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests or someone else's interests and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- Making a decision about your recruitment or appointment.
- Checking you are legally entitled to work in the UK.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Complying with Safer Recruitment obligations.
- Complying with health and safety obligations.
- Where the position is exempt from the provisions of the Rehabilitation of Offenders Act 1974
- To prevent fraud.

We are allowed to use your personal information in this way to carry out our obligations where posts involve contact with children or vulnerable adults or groups such as the infirm, elderly or mentally ill.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with other third parties including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Sharing personal data with third parties

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents). The following third-party service providers process personal information about you for the following purposes:

Names of Providers	Activities carried out
Royal London Pension Benefits	Pension Provider
JMV Solutions Ltd Data Security	Data Storage
Scottish Engineering	Employment Law Advisory Service
U-Check	DBS Check
Care Check	DBS Check
IMASS (Medigold Health)	Occupational Health
Care Friends	Recruitment

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We will share your personal information as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Care Quality Commission

The role of the Care Quality Commission (CQC) is as an independent regulator. It registers all health and social care providers in England and it inspects such establishments to ascertain whether or not standards are being met. The CQC uses personal data to help them carry out their role as regulator. For more information on how the CQC might use personal data, please see their privacy statement https://www.cqc.org.uk/sites/default/files/20151029_CPI_leaflet.pdf

Data security

We have put in place measures to protect the security of your information. Details of these measures are available in our Information Security Policy which is available on request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

They will only process your personal information on our instructions and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from Jill Barbour, Data Protection Lead. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of

your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the organisation we will retain and/or securely destroy your personal information in accordance with our data retention policy.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact Jill Barbour, Data Protection Lead in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. This will be assessed on a case by case basis.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Lead. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Lead

We have appointed Jill Barbour, Data Protection Lead to oversee compliance with this privacy notice.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Concerns

If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Lead. You have the right to make a complaint at any time to

the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact Jill Barbour, Data Protection Lead on 01752 546449 or email jill.barbour@beyondlimits-uk.org

People We Support Privacy Statement

Scope

Beyond Limits is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

Responsibilities

Beyond Limits are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to all the people Beyond Limits support and have supported. This notice does not form part of any contract to provide services. We may update this notice at any time.

It is important that we help you and/or your guardian/appointee to understand this notice so that when we are collecting or processing personal information about you, you are aware of how and why we are using such information. We will do this in a way that makes sense to you.

Privacy notice

You can contact your Service Leader about this notice or our Data Protection Lead can be contacted directly here:

- jill.barbour@beyondlimits-uk.org
- 01752 546449

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

Your Personal Data

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data)

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance Number, Hospital Number and NHS Number.
- NHS Hospital Passport

- Benefits information (where applicable).
- Copy of driving licence (where applicable).
- Matching information for recruitment purposes.
- Photographs (where applicable).
- Personal Money Receipts/Records/Bank Statements (where applicable)
- Service Design, Working Policy, Daily Notes, Safety Assessments, Meeting Notes.
- MAR Sheets, Accident and Incident Reports, NHS & Medical Records and Safeguarding Alerts.
- Mobility Documents and Mileage Books.
- Criminal convictions and offences (where applicable).

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract of support that we have with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

Use of your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract of support with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

Supporting you to make decisions about:

- Your team recruitment
- How we can work best for you
- Your planning day, service design and working policy

Providing the following benefits to you:

- Liaising with all necessary stakeholders
- Administering the contract of support we have entered in to with you
- Safeguarding your best interests whilst maintaining your privacy
- Achieving your chosen outcomes
- Complying with health and safety obligations
- To prevent fraud

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of you and your team).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

In limited circumstances, with your explicit written consent.

Where we need to carry out our legal obligations and in line with our data protection policy and/or other policies.

Where it is needed to assess your capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as a Service Provider

We will use your particularly sensitive personal information in the following ways:

- To inform your Service Design and Working Policy
- To record/report Accident and Incidents
- To record/report Safeguarding Alerts
- To help you recruit appropriately matched staff

Consent

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our contractual obligations as your service provider. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data.

If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Data Sharing

We may have to share your data with third parties, including third-party service providers e.g. your funders. We require third parties to respect the security of your data and to treat it in accordance with the law.

Sharing personal data with third parties

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Data security

We have put in place measures to protect the security of your information. Details of these measures are in our Information Security Policy which is available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees who have a business need to know.

They will only process your personal information on our instructions and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

When we are supporting you to travel to/from your GP/Hospital or any other appointment which requires your NHS Hospital Passport we will carry this sensitive document in a secure, wearable document wallet to ensure its security.

Any deviation to this protocol must be approved by your Service Leader and fully documented in your Working Policy.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from our Data Protection Lead. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. If we no longer support you then we will retain and/or securely destroy your personal information in accordance with our data retention policy **OR** applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact your Service Leader.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. This will be assessed on a case by case basis.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact your Service Leader. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Lead

We have appointed a Data Protection Lead to oversee compliance with this privacy notice.

Concerns

If you have any questions about this privacy notice or how we handle your personal information, please contact your Service Leader You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact

Jill Barbour - **Data Protection Lead**

jill.barbour@beyondlimits-uk.org

01752 546449