



Data Protection

Privacy Policy

1.0 The purpose of this policy

Let's Enable is registered at 98 Warwards Lane, Birmingham B29 7RD. Let's Enable is a CIC that needs to retain and process certain data to enable the efficient running of the business and for health and safety purposes. This includes personal data on volunteers, employees, customers, parents, carers and service users. Let's Enable is committed to protecting all personal data. We are committed to complying with privacy and data protection laws and being transparent about how we process personal data. This policy outlines our views and practices regarding your personal data and how we will treat it.

1.1 The principles of General Data Protection Regulations (GDPR) are that personal data is:

- Only used for the purposes agreed to by the data subject, at the time that they gave the information and not used for any other purpose
- Adequate and limited to what is necessary
- Accurate and kept up to date
- Retained for only so long as necessary
- Processed in a way to ensure security
- Accountability.

1.2 GDPR places emphasis on:

- Reviewing approaches to govern and manage data protection
- Providing individuals with more information about their personal data
- Individuals rights about their personal data
- Individuals have the right to access and receive a copy of their personal data, and other supplementary information
- Obtaining consent
- Breach notification duty



- The GDPR's transparency requirements are integral to the ability to provide informed consent. This entails transparency about the information to be provided and permissions required from individuals to justify use of their personal data.

1.3 List of individual rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in automated decision making and profiling.

Let's Enable will:

- Ensure GDPR policy and procedures are up to date and communicated clearly – for example to staff and volunteers
- Provide team GDPR training to staff and volunteers where appropriate
- Only keep personal data for as long as it is relevant to the purpose for which it was collected or for as long as we are required to keep it by law
- Ensure that all staff, volunteers, parents and carers respect data privacy
- Let's Enable will protect data with robust security measures and be honest in what we hold
- Not keep more information than we need, always provide or remove data on the request of the data owner and always react to any information we receive from the Information Commissioners Office (ICO)
- If information is requested Let's Enable has 30 days to provide information
- Data breaches will be reported to the Information Commissioners Office (IOC) and the data owner within 72 hours of identification of the issue



- <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>.

1.4 Key legislation and regulations related to the GDPR

- General Data Protection Regulations (GDPR) 2018
- CQC Regulation 17 – Good Governance
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Standards for Professional practice.

2.0 Types of data and information collected

2.1 Why do We use the personal data?

Let's Enable uses the personal data you provide to us for the following purposes:

- To provide you with billing information in relation to any services that we provide to you
- To notify you about changes to Our Services. This is necessary for the performance of the Agreement we have in place with you
- To prevent or investigate prohibited activity.
- To enforce Terms and Conditions and/or any Agreement entered into between us.
- To obtain consent for participation in activities by the service user or parent/carer for different types of activities.

We may collect your personal data in different ways, for example:

- When you, your parent/guardian/carer, teacher, or health care professional communicate with us by post, telephone, SMS, email, social media or via our website



• From the information you provide to us when you make an application to work for us, or from third parties such as your previous or current employers so we can verify details about you. This includes information from the Disclosure and Barring Service

- As you interact with us in other ways; e.g as a contractor, or in any other capacity
- Consent forms - Contact details such as name address, email address and phone numbers
- Date of birth
- Qualifications
- Name of your parent/guardian/carer (if you are under 18) or do not have the mental capacity to consent
- Name and contact details of any next of kin for use in emergencies
- Any Special Educational Needs (SEN) requirements including relevant medical records detailing conditions and medications
- Child/adults individual behaviour plan – helps Let’s Enable to recognise and respond to behaviours and have strategies in place to help the individual. This is agreed with parents/carers and health care professionals (if appropriate)
- Medical details, parents and carers emergency contact details – may include activities the individual should not take part in and who to contact in an emergency. This helps Let’s Enable tailor sessions to suit the needs of the client and is in the best interest of the client’s physical and mental well-being. It is essential that we know about potential conditions and triggers so we can minimise risk and have strategies in place with parents and carers in case this does occur
- This could also include Let’s Enable approaching health care professionals, such as the General Practitioner, Physiotherapist or Occupational Therapist to gain more information. For Personal Training sessions this could include a General Practitioner’s referral. Our legal basis for using your personal information in this way is for the health and safety of the client and to improve or services and ensure effective performance of the contract
- Information about sessions are kept so Let’s Enable can establish goals for service users and show progress and activities they liked/disliked helping maximise enjoyment during sessions. This is of benefit to the service user and case studies can be used for funding applications (with consent)



- By submitting your or anyone else's data to us, you must ensure that you have full authority and consent to supply us with that data on their behalf and you warrant to us that you do have that authority.

2.2 How long do we hold personal data

Let's Enable will keep personal data for as long as we have an agreement between Let's Enable and the service user, parent, carer, volunteer, or employee. We will keep your personal data for as long as we have an agreement to provide services to you. If the service is stopped, we will delete your personal data, except where we need to keep it for legal, regulatory or audit reasons, in which case we may do so for 6 (six) years after you cease to be our customer. Let's Enable will handle, store and dispose of data responsibly and securely.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you. Otherwise, we will only retain your personal data for as long as is necessary for the reason we collected it. In making this decision, we consider the amount, nature and sensitivity of the data, the reason we process it and, whether we can achieve that purpose without processing your data, legal requirements, and the potential risks to you from us processing your data.

2.3 Employment

We have policies, procedures and training in place to help our employees and volunteers understand their data protection responsibilities and follow the data protection principles. Let's Enable only collects the information needed for recruitment purposes as part of the job or volunteer application process, such as your name, address, email address, phone number, employment history, salary history and referees. We will retain Recruitment Data for as long as is necessary, and in any event for no longer than 2 (two) years, and, if we employ you, for the duration of your employment with us and for a period after your employment ends. We will use Recruitment Data only for the purpose of dealing with your enquiry or application, or to fulfil our legal and/or regulatory obligations. This might include contacting you to keep your application moving and assessing your suitability for the particular role we have available. We will not share Recruitment Data with any third parties for marketing purposes. You do not have to provide personal data to us when we ask for it, but it may



impact your application if you do not give us all of the information we need to assess your suitability for the role available. If we make you a conditional offer of employment, we will ask you for further information, such as proof of your qualifications and identity. If we then make you a final offer of employment, we will

ask you for details of your bank account (so we can pay your wages), emergency contact details, and details of any pension scheme of which you are a member. We process employee personal information to fulfil our contracts with our employees and meet our legal obligations as an employer. We are required by law to share some financial information with the HMRC. Our legal basis for using your information for this is for the performance of a contract. We may use your personal data to comply with subject access requests; tax legislation; for the prevention and detection of crime; and to assist the police and other competent authorities with investigations including criminal and safeguarding investigations.

All employees and volunteers must comply with this policy, failure to comply with this policy may result in disciplinary sanctions, up to and including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

2.4 Where We store your Personal Data

All information that you provide to Let's Enable is stored on secure devices. Unfortunately, the transmission of information via the Internet is not completely secure. Although we do our best to protect your personal data, we cannot guarantee the security of your data transmitted to the Website. Any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access. We ask that personal and sensitive data is not sent via the website.

We hold all personal data securely, whether the personal data is in physical or electronic format. Let's Enable limits access to personal data to those employees, volunteers, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.



2.5 Data Retention

There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business. This covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents and audio and video recordings. It applies to both personal data and non-personal data. This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices.

2.6 Sharing personal information

We will only share your personal information where we are required to fulfil our contract with you, or legitimate interest, where we have your consent, or we are required to do so by law. Our legal basis for the purposes that we process personal information is for the performance of a contract, or for our legitimate interests or consent. We may collect and use your personal data if it is necessary for our legitimate interest and so long as its use is fair, balanced and does not unduly impact your rights. We will ask for your consent to send you marketing emails and text messages. You can withdraw consent for this at any time. In an emergency situation we may need to share your personal details, for example, the emergency services.

3.0 Dealing with complaints and appeals

If a complaint or an appeal is raised with us, we will process the personal information that is provided to us to manage and resolve the complaint or appeal. This may include sharing relevant information depending upon the nature of the complaint and the area it relates to. Our legal basis for using personal information for this purpose is to fulfil our legitimate interest and fulfil our objective of resolving complaints in a careful and appropriate manner.



4.0 Undertaking safeguarding activities including DBS checks and casework

When necessary, we process relevant personal information about members, volunteers, service users and employees for safeguarding purposes. This might include undertaking DBS and other checks to identify any criminal and other activity we need to be aware of and casework. It may be necessary to share some personal information with relevant authorities such as the police, Social Workers, health care professionals and the local Safeguarding Team. Our legal basis for this processing is to meet our legal obligations.

5.0 Contact

Questions, comments and requests regarding the data protection policy are welcomed and can be sent to us directly via email, website or by post sent to our registered address. Please note, do not send personal or sensitive data through the website.

Nina Linzell serves as our Data Protection Lead. If you have any questions regarding our Privacy Policy, please email nina@letsenable.co.uk.

General Commissioners Office

If you are not satisfied with our response to any query you raise with us, or you believe we are processing your personal data in a way which is inconsistent with the law, you can complain to the Information Commissioner's Office whose helpline number is: **0303 123 1113**.



This policy will be reviewed annually

Date 26/01/2024

Signature 

Print Name Nina Linzell

Next review date:

26/01/2025