# DATA PROTECTION AND PRIVACY STATEMENT

## ABOUT EDEN FUTURES

Eden Futures is the name given to a group of four companies who provide social care to individuals. The four companies are as follows:

**Eden Supported Living Ltd** (Company no-07276039)

**Housing and Support Solutions Ltd** (Company no-04383479)

**Supported Homes Ltd** (Company no-05760518)

**Essential Futures Ltd** (Company no-04541238)

Within this statement, a reference to company will include all of the companies named above.

All companies named above are registered with the Information Commissioners Office (ICO) for data protection purposes.

## THIS STATEMENT

The purpose of this statement is to provide information on the control, processing and use of data within the company.

## ABOUT PERSONAL DATA

Personal data is information held by the company that would enable the identification of a living individual.

The actions of the company meet the requirements of the Data Protection Act 2018 (incorporating the principles of the General Data Protection Regulations 2018).

## INDIVIDUAL RIGHTS

The company will uphold and support all individual rights of data subjects under the General Data Protection Regulations. All data held will be stored securely and the privacy and confidentiality of data subjects will be a priority in all data processing. Data will not be held for any longer than is required.

## HOW THE COMPANY COLLECTS DATA

Data is collected and held through all company business activities. This means data is collected by doing the following –

- Retaining details when someone makes an enquiry about services provided by any of our companies.
- Assessing an individual prior to formally providing support.

- Developing and retaining records in respect of people supported. This may include details of others involved, including external professionals, regulators and relatives.
- Creating records throughout the recruitment process (see Appendix A
- Utilising information provided in order to maintain staff employment – including the payment of salaries.
- Meeting legal and regulatory requirements such as (but not limited to) reporting to HMRC, HSE, DBS and the Care Quality Commission.
- Seeking payment for services that have been delivered by the company.
- Making payment to contractors or others for services delivered to the company.

## THE DATA COLLECTED BY THE COMPANY

The data collected depends on the reason that for collecting it. It can include, but is not limited to, the following –

- Names, addresses, email addresses and telephone numbers.
- General employment information, including bank account details. This can include sensitive personal data in relation to health and DBS identified risks in addition to ongoing employment information such as information related to training, performance and disciplinary action.
- Recruitment information for people wishing to work for the company (see appendix A).
- Information collected during the assessment of an individual in relation to potentially providing a service. This can include sensitive personal data in relation to health or protected characteristics.
- Medical information relevant to the role of staff or the support provided to an individual.
- Other records related to the support of individuals including information received from external professionals directly involved in that support.
- Audit data.
- Financial information to enable invoicing for services provided and payment of services received and other financial information related to the company.

The legal basis on which the company relies in order to collect and process data under the GDPR/Data Protection Act 2018 is that of legitimate interests, consent and contractual obligations.

## WHAT DATA IS USED FOR.

The company collects data to fulfil its' business function and contractual obligations. These include, but are not exclusive to:

- To enable appropriate support to be provided to individuals to enable their outcomes to be achieved in addition to company contractual arrangements with local commissioners.
- Providing information on services or ways in which a service user can be supported.
- Managing the employment of staff including the recruitment of staff (Appendix A) and their exit from the business in additional to their ongoing work.
- Keeping records to enable care and support to be delivered to service users.
- Fulfilling and evidencing regulatory and contractual requirements.
- Sending marketing information where consent has been provided.
- Seeking feedback from relevant parties where consent has been provided.
- Photographs of individuals or groups may be used as marketing material with consent.
- Employee contact information and records of their working patterns and locations will be provided to NHS Test and Trace if requested to do so.

Information will only be used for the purpose for which it is provided. If the company wishes to use data for any other purpose, express permission will be sought to do so.

In the event that the company is asked to provide information to prevent immediate harm or is asked by the police to provide information in respect of a criminal investigation, it will act in accordance with its' responsibilities as set out in the General Data Protection Regulations.

## SECURITY OF DATA

All electronic data is held securely within company systems with appropriate security measures in place to ensure that the information is both securely stored and that permissions are in place to ensure that only employees with a "need to know" information have access to stored information.

All paper records are held securely in locked cabinets with key access restricted to those who require those records as part of their job role.

## IMAGES AND SOCIAL MEDIA

If any person responds to the Company on Facebook or Twitter, that information may be shown on our website.

The Company monitors comments on social media and will act in respect of these comments where appropriate.

Images of people will only be used on our website or in any other marketing material if permission has been given for the company to do this.

## INFORMATION FOR MARKETING PURPOSES

The company may wish to advise interested parties of new company initiatives that could be of interest. Consent will be requested to do this, and information will not be sent to anyone who has not consented.

## WHO CAN ACCESS INDIVIDUAL DATA?

A person's data will only be accessed by individuals within the company who need to do this in order to complete their work for the company.

The company contracts with external companies to provide IT services. All of those companies are required to be compliant with GDPR and have provided assurance that this is the case.

## SUPPORTING INDIVIDUALS WHO CANNOT CONSENT

The company provides support to a number of individuals who do not have the capacity to consent to the use and storage of their personal data. In this instance decisions about data use and storage will be made on a Best Interest basis in line with the requirements of the Mental Capacity Act 2005.

## TESTIMONIALS

From time to time the Company may use direct feedback from individuals in receipt of services or others who have an interest in how the Company performs. This may be published on the Company website, contained in marketing material or shared with a commissioner or regulator. This information will not contain any information which could enable the identification of the person sharing it.

## DATA RETENTION AND SECURITY

Different types of data are retained for different periods of time in line with regulatory and best practice guidelines. Data is not retained for any longer than is required and this is regularly reviewed. Full details can be found in the company Archiving Policy which can be provided on request.

## COVID 19

The GDPR are still in force during the Covid-19 pandemic. However, there may be some circumstances where the government has set up systems to manage the pandemic where information will be requested in very specific circumstances

## NHS TEST AND TRACE

In the normal course of business, the company will be provided with contact details of any visitors to company offices. If the visitors are not regular company partners or contacts, the company will retain the contact details for 21 days before deleting, in accordance with government guidance.

## OTHER

Appendix A contains information about the National Patient Data Opt-Out and Appendix B contains information about data held in relation to recruitment. This information is also available when applicants log onto the company recruitment portal.

## HOW TO CONTACT US

If you wish to make a request to see data held by the Company about you, please contact the Company and provide – Your full name and address; your email address if you have one and any other contact details. You must provide details of your enquiry.

The Company head office is –

**Eden Futures**

**17a Friary Road**

**Newark**

**NG24 1LE.**

**03300 240 039**

You can email GDPR@edenfutures.org with any queries in respect of Data Protection and how the Company collects, uses and stores data.

The person who is the Data Protection Officer for the Company is Sarah Frank, Director of Quality and Compliance.

If you wish to see a full version of our Data Protection Policy, please contact us as above.

The version of this statement on the website will always be the Company's most recent statement in respect of its approach to the GDPR and the management of data within the Company.

This statement confirms that the company will commit to being compliant under the General Data Protection Regulations (EU) 2016/679 and the Data Protection Act 2018.

## APPENDIX A

# National data-opt out statement – people we support

Under the national data opt-out everyone who uses publicly-funded health and/or care services can stop health and care organisations from sharing their "confidential patient information" with other organisations if it is not about managing or delivering their own care. For example, if this information is used for research or planning purposes.

Information may be shared with other organisations, if this is required to manage someone's care. Information may also be shared if explicit consent has been given in respect of sharing that information or if the information is appropriately anonymised so that any individual is not identifiable.

Most care providers do not share confidential patient information except for the purpose of managing or delivering care.

At Eden Futures we do not share any information that we collect about service users and their care and support except for the purpose of providing that care and support. It is only shared with people who "need to know" this information in order to support the care being provided and staff at the company work under strict Confidentiality and Data Protection policies.

There may be exceptions in relation to legal and public interest requirements where there may be an obligation to share information externally, and these are detailed in our Data Protection Policy.

We are using the term "confidential patient information" as this is the term already used by the NHS where the opt-out is already in force. "Confidential patient information" applies to information about someone's health *or* social care that can identify them.

Service users will also be asked about this opt-out by other healthcare providers such as their GP practice or when in receipt of acute NHS services (such as in hospital). It is the responsibility of that provider to ensure information is provided in relation to any information held by those parties.

If service users or their relatives or representatives have any questions about the national data opt-out choice at any time, there is an online service to contact as follows: www.nhs.uk/your-nhs-data-matters/ or they can call this number 0300 3035678 – for further information.

All companies within the Eden Futures Group that provide support to individuals are registered with the Information Commissioners Office. In addition companies are registered for the NHS Data Security Protection toolkit and have achieved compliance with the required standards.

## APPENDIX B

## Recruitment of Applicants

This appendix sets out the basis on which the company collects, uses, shares and disposes of information provided by job applicants. The job applicant retains all existing rights under GDPR/Data Protection Act 2018 in relation to this data.

In making an application to join the company, the applicant consents to the collection, use, sharing and disposal of information provided by themselves or created by the company in relation to their application. All information is provided on a voluntary basis by the applicant. If the applicant does not wish to provide relevant information they may choose not to do so, but this may impact on the progression of their application.

## WHAT INFORMATION DOES THE COMPANY COLLECT AND HOW DOES IT DO THIS?

The company will collect a range of information about you in the course of your job application. This may include (but is not limited to):

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information from interviews and phone-screenings you may have;
- information about your current level of remuneration, including benefit entitlements;
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

This information may be collected in a variety of ways – such as through an application form or CV; by the applicant providing documents (such as identity documents); information collected through the assessment process including interview records and other assessment information.

We may also collect personal data about you from third parties, such as references supplied by former employers. We will seek information from third parties only once a job offer has been made to you and with your explicit consent (stated on the application form) that we may do so.

Data will be stored in a range of different places, including on your application record, in our HR management systems and our email system.

## WHY DO WE NEED TO PROCESS YOUR PERSONAL DATA THROUGH THE RECRUITMENT PROCESS?

There are a number of reasons for this:

- The management and tracking of applicants through our recruitment process. This enables us to contact and update you, make arrangements for interviews and give you the outcome of the process.
- We retain information from unsuccessful candidates for a period of time in order to respond to any questions and provide information to defend any legal claims.
- We have a legal obligation to confirm identity and that applicants have the right to work in the UK and this must be done prior to the commencement of employment.
- We want to ensure that any appropriate reasonable adjustments are applied to applicants and new employees.
- We may process special categories of data such as information about ethic origin for monitoring purposes in relation to equal opportunities.

Your data is only used for the purpose for which it is provided – namely the recruitment process and on-boarding of successful candidates who accept a role with the company.

## WHO CAN ACCESS MY DATA?

Your information will only be viewed or used by those in the company who are involved in the recruitment process. This includes, but is not limited to, the following:

- Those employees who work in the HR and Recruitment departments.
- Members of the IT team who may support in the recording of data and management of systems that store it.
- Managers who are directly involved in recruiting staff and who interview candidates and make decisions on suitability for employment.
- Senior company managers who may need to review processes in the event of a concern.

- If you receive and accept an offer of employment, we will then need to share your information with external parties such as previous employers/personal references and DBS authorities to complete the necessary DBS, Adult First or Children DBS checks as applicable to the role.
- We may need to share your data to comply with a legal request – for example from the police.

## HOW LONG IS MY DATA RETAINED FOR?

If you are a successful candidate and join the company, your initial data forms part of your employee record and therefore becomes subject to the retention periods as stated in our Archiving Policy.

If you an unsuccessful candidate, your data is retained for a six month period in case of any question following the conclusion of the recruitment process. In rare situations we may retain data for longer but will only do this if there is a specific and documented reason to do so (for example, to defend a legal claim).

## OTHER INFORMATION

As soon as we collect your data you have all individual rights as stated in the GDPR and Data Protection Act 2018. If you wish to exercise any of these rights please as a result of your recruitment application, please contact GDPR@edenfutures.org setting out your request.

By entering into the company recruitment process and providing personal and other data on a voluntary basis, you are providing consent for the use of that data as set out in this statement. If you refuse to provide any data requested that will impact on our ability to proceed with any application or employment offer.

If you require further information about the use of data within the recruitment process, please contact GDPR@edenfutures.org or contact a member of the company recruitment team.

.