DATA PROTECTION POLICY

POLICIES AND REGULATIONS

- General Data Protection Regulations (GDPR) (EU) 2016/679
- Confidentiality Policy
- Record Keeping Policy
- Document Management and Key Security Policy
- Subject Access Request Policy
- Data Breach Policy
- Support Planning Policy

SCOPE

This policy applies to all activities of the following companies – Eden Supported Living Ltd; Housing and Support Solutions Ltd; Essential Futures Ltd and Supported Homes Ltd. Collectively these Companies are known as Eden Futures and any reference to Company within this policy will apply to all of these companies.

This policy applies to all individuals who work to deliver the activities of the company. This will include (but is not limited to) all employees but also contractors, students and volunteers.

This policy applies to all geographic areas in which services are delivered.

All companies named in this policy are registered with the Information Commissioners Office in line with Data Protection legislation.

POLICY STATEMENT

In order to carry out its business, Eden Futures needs to collect and use information provided by individuals. This is in relation to ensuring that regulatory requirements are met; staff are recruited, supported and paid for their work; contractual obligations are met; service users are provided with support and the company is paid for the services it provides. It also applies to other individuals that the company may have a relationship with – such as relatives or other stakeholders.

This policy will describe how this data must be collected, handled and stored in order to comply with the law.

OBJECTIVES

This policy will ensure that Eden Futures–

- Meets its' legal obligations under the General Data Protection Regulations (GDPR).
- Obtains, holds, uses and shares information only in line with the responsibilities and actions identified within GDPR.

- Protects the rights of staff, service users and other stakeholders in respect of their data.
- Is open about how it stores and processes the data of individuals.
- Protects itself from the risks of a data breach.
- Makes staff aware of their personal responsibility to manage data in a way that protects confidentiality is in accordance with GDPR requirements.
- Identifies the rights of individual data subjects.
- Protects the personal data of vulnerable service users through appropriate management in accordance with the law.

PRINCIPLES OF DATA PROTECTION

The principles of data protection are set out below. Data must be –

- Processed fairly and lawfully.
- Be obtained only for specific and lawful purposes.
- Be adequate, relevant and not excessive.
- Be accurate and kept up to date.
- Held only for the time it is needed and not for any longer than necessary.
- Be processed in accordance with the rights of data subjects.
- Be protected in appropriate ways.
- Retained within the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection (check this out).

DEFINITIONS UNDER GDPR

Key definitions under the General Data Protection Regulations are the following:

- **ICO** – Information Commissioners Office. This office of government oversees the implementation of data protection legislation. Significant breaches in data protection have to be reported to the ICO. They can impose sanctions on companies and organisations who do not comply with the law. They can be contacted on www.ico.org.uk
- **Data Controller** – A data controller determines the purposes and means of processing personal data. Eden Futures is a data controller for the purposes of the regulations. A data controller is responsible for ensuring that any contracts taken out with data processors comply with the GDPR.
- **Data Processor** – A data processor is responsible for processing personal data on behalf of a data controller. There are specific legal obligations on a processor under GDPR. They must maintain records of personal data and processing activities and have legal responsibility for any breach of that data.
- **Data subject** – Any person on whom data is held by the company or data processor contracted to the company.
- **Lawful Basis** – there are six lawful reasons which enable the company to process data and they are detailed in the section below.

- **Privacy notice** – a notice which identifies the company and provides information about how the company intends to use any information given to it. This will include data retention periods and the rights of the individual to complain to the ICO.
- **Individual rights** – these are explained in the appropriate section of the policy.
- **Consent** – the law says that consent cannot be conferred through inactivity or silence, it must be freely given and a positive opt-in. It also says that it must be separate from other terms and conditions and that the withdrawal of consent must be simple. Consent has to be verifiable – this means that it must be able to be checked.
- **Data Breach** – this is where some personal information on an individual, or group of individuals, has been disclosed to others who have no right to have access to this information. This could range from the inappropriate sharing of a single piece of information, to a widespread breach of data through access to electronic systems. The company will comply with all ICO processes and guidance in respect of data breaches. See section within this policy.
- **Data Protection Impact Assessment** – the company has carried out a Data Protection Impact Assessment which identifies all data requested, used and processed within the organisation or by an external party. It has considered the impact of any breach of that data and the methods to be used to prevent such a breach. The company considers this to be a live document, and, as such, will keep it under continuous review.
- **Data Protection Officer** – this is an individual identified by a company to take responsibility for data protection within the organisation and to ensure that the company is aware of any risks in respect of data. They will provide information to the Directors and Board of the company and advise staff members in respect of any actions. Eden Futures does not have a legal requirement to identify a Data Protection Officer but believes that it is best practice to do so. **The Data Protection Officer for the organisation is Sarah Frank who holds the position of Director of Quality and Compliance.**

THE LEGAL BASIS FOR PROCESSING INFORMATION

There are six areas to consider, any of which will supply a legal basis for the company's right to process information –

- **Consent** – the individual has given clear consent for the company to process their person data for a specific purpose.
- **Contract** – the processing is necessary for a contract the company has with an individual or because they have asked you to take specific steps before entering into any contract.
- **Legal obligation** – the processing is necessary for the company to comply with the law (outside of any contractual obligations).

- **Vital Interests** – the processing is necessary to protect someone's life.
- **Public task** – the processing is necessary for you to perform a task in the public interest or for your official functions and the task or function has a clear basis in law.
- **Legitimate interests** – the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

DATA PROTECTION RISKS

When any data is stored or collected for any reason there are risks attached to this. They are as follows –

- **Breaches of confidentiality** – information is given to those who have no need or right to know that information. In extreme cases the information given could be used inappropriately.
- **Failing to offer choice** – individuals should be free to decide how a company uses data relating to them and a breach of data removes or diminishes that right.
- **Theft of data** – this might be for criminal or other purposes but could result in significant detriment to an individual or group of individuals.
- **Reputational damage** – the company and its' reputation may be damage if information is stolen from them or inappropriately shared. This will be the case irrespective of any detriment to an individual or group of individuals.

INDIVIDUAL RIGHTS UNDER GDPR

Under the regulations, individuals on whom the company holds data, have specific rights. These are the following –

- The right to be informed.
- A right of access
- A right to rectification.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making – including things like profiling.

The company's Subject Access Request Policy provides detailed information to individuals about how they can request to see and take action in respect of information held on them and information on data and individual rights and actions is also within the Employee Handbook.

STAFF GUIDELINES IN RESPECT OF DATA PROTECTION

Staff have a responsibility to ensure that any data they handle is done so appropriately and in line with company policies in order to prevent any breach of that data. These responsibilities are as follows –

- The only people able to access data used by the company are those who need to do so in order to carry out their work.
- Confidential data should not be shared informally – employees should ensure that they follow guidelines at all times.
- The company will provide training to ensure that employees are aware of data protection responsibilities.
- Employees must follow the **Documents Management and Key Security Policy** in respect of day to day use of documents and information within the company. This is available on the company intranet.
- Personal data should not be disclosed to unauthorised people either internally or externally and staff have a responsibility to ensure that they know who they are sharing service user data with and that the person has a "need to know" this information. Further information is contained within the **Company Confidentiality Policy.**
- Staff should reduce the amount of personal information that is printed and must ensure that they remove the document from the printer immediately after it is printed.
- If printing is necessary, staff must ensure that any printing is sent to the correct printer. This applies in company offices where a printer selection is available to staff. Printing must be done in proximity to the person requesting it.
- Once any document is no longer needed it must be shredded or placed within the secure shredding boxes held in regional offices.
- Strong passwords **MUST** be used on company systems and they must not be shared. If staff are provided with a default password to access a system, they must change this at the first opportunity. Please see Appendix A for further information.
- Staff must **NEVER** attach their password or access code to any device.
- Employees must use any measures provided by the company to support data protection. This includes following advice from the IT department in respect of security of laptops, chromebooks, desktops and phones, as well as using other equipment provided.
- Any employee who is likely to use a company laptop in a public place (such as a train or a hotel) must request a privacy screen from the company IT department.
- Any employee who, through their role, travels with a company phone and laptop, must be vigilant at all times in respect of the security of those items.

Laptops or phones should never be left in a car, even for a very short period of time.

- Employees must follow company guidance in respect of record keeping in order to further protect the confidentiality of individuals in receipt of support.
- Employees must act in line with the **Archiving Policy** and dispose of information that is no longer in use. This means that all information should be regularly reviewed and updated, and old information should be disposed of.
- Information that is locked away must only be accessed by the keyholder.
- Any individual who does not have a professional relationship with the company must not be given company information to transport. This does not apply to the delivery of individual employee information (such as timesheets, sick notes) delivered with the employee's permission by someone such as a family member.
- Employees can seek advice from their line manager or the company Data Protection Officer if they are unsure of any aspect of data protection and what they need to do to be compliant.
- The Company will regard any breach of data protection as a very serious matter. If staff are found to be in breach of any policy in relation to data protection, disciplinary action may be a consequence

DATA USAGE

The Company utilises a range of methods to ensure that its usage of data is secure and data privacy is protected. These include the following –

- Company phones issued to staff have to be set up with a PIN number known only to the member of staff.
- Laptops are encrypted.
- Email attachments are encrypted.
- All systems within the organisation are set up on a permissions basis which is managed and monitored by the IT department. These permissions are based on the role of the employee within the Company. Permissions cannot be changed by staff members who have no authority to do so.
- Any external platform used by the company, which links to internal systems, will have permission-based access which is restricted to those individuals who need the information contained as part of their job role.

DATA ACCURACY

The law requires that a company takes reasonable steps to ensure that data is kept accurate and up to date. It is the responsibility of all employees who work with any data, to take reasonable steps to ensure that it is kept as accurate and up to date as possible. This will be achieved by taking the following steps –

- Data should be held in as few places as necessary. Staff should not create any additional unnecessary data.

- Staff should take every opportunity to ensure data is updated. For example, a manager could ask a staff member in supervision if there is any change to their personal details and then action this.
- The company will do everything it can to ensure that it is straightforward for data subjects to update their information where necessary.
- If an inaccuracy in any data is discovered, the data should be updated at the time.
- Staff must remove out of date information from service user files as this increases the likelihood of inaccurate information be shared.

COMPANY SYSTEMS

In addition to records held within files and on paper, the company uses a number of electronic systems to manage and support its' day to day operations

- **ERIC** – electronic system for recording events. All staff can access the ability to report an event, but access to read and review events is limited to a permission-based system. Staff have certain levels of access which determine the actions they can take and then the permissions they are granted will allow them access to services. This permission is determined by their work role and the services which are relevant to that.
- **ERNIE –** this is the Company intranet. Staff access through a link on the company website and access is password protected. Staff cannot alter content that is on the intranet.
- **HENRY –** this is the Company Human Resources system (Zoho People). This holds personal data on all employees of the Company. Access to this system is based on permissions with access limited to those who need to know the information to perform their job role.
- **CRM** – This is Zoho CRM and it's purpose is to record all properties and services within the Company. Access is permission based in line with the job role of the person.
- **TEAMWORK PROJECTS** – this is a cloud-based project management system. Access is limited to those working on specific projects.
- **OFFICE 365 –** this includes sharepoint (on which documents are stored). Access is limited to those with appropriate permissions and is in relation to their job role.
- **LIFEWORKS –** this is an employee welfare and benefits platform accessible to employees by an app on their personal phones. Contact information is stored by Lifeworks only for those employees who have given their express consent and participation is voluntary. Employees cannot view the information of any other individual.
- **CARESHIELD –** this is the Company e-learning platform. Access is based on permissions and employees can only access information related to training for their job role.

- **PAN-INTELLIGENCE –** this is a system to bring together financial data and utilise it to support the business functions of the company. Access is based on permissions related to the job role of the employee and the information needed to support that role.
- **FILE SERVER DRIVE MAPPING –** servers are being phased out with the exception of some finance related usage. Access will be based on permissions in line with the job role of the employee.
- **MALINKO –** this is a rota writing platform which pulls information from Zoho CRM and Zoho People. The system uses an Application Programme Interface to "talk" to the Zoho systems and gain the information it needs to support the function it provides. Information is encrypted, and staff have access to information based on the services they manage.
- **CARBONLABS –** this takes information from Zoho CRM in order to support the function of the auditing of specific areas of service delivery.

SERVICE USER DATA

The company will have a great deal of data on individuals to whom it provides support services. This is held on paper records within files in both services and offices, and also electronically. This data will be managed in line with all other data within the organisation.

Staff will ensure that the consent of any service user is provided for the use of their data in any records held. This can be recorded within the "Recording" section of any Outcome Focused Support Plan developed for an individual, or by means of an overall consent form signed by the service user and placed at the front of an individual's file. The ability to give consent will be determined by the capacity of the individual and if a service user cannot consent then it will be considered through the MCA and Best Interest process that takes place in respect of consent to their care and support.

If a service user with capacity refuses consent for data to be held on them, the company will not be able to provide a service to that person. This will need to be discussed and agreed during the process of assessing an individual prior to receiving support from the Company.

SUBJECT ACCESS REQUESTS

This is the legal right of an individual data subject to -

- Ask what information the company holds on it and why.
- Ask how to gain access to it.

Detailed information about how to make such a request is held in the **Data Protection – Subject Access Request Policy.** Further information can be obtained from the Human Resources Department of the Data Protection Officer.

DATA BREACH

The company fully understands its' responsibilities in respect of any breach of personal data. Detailed information is held in the company **Data Protection – Breach of Personal Data Policy.**

WEBSITE STATEMENT

A statement has been placed on the company website which summarises how the company meets the General Data Protection Regulations and to provide information on how any party can contact the company with a query about their data or a request to access it. That statement will be reviewed annually (or more frequently if needed) alongside this policy.

TRAINING AND INFORMATION

The company will ensure that all employees are aware of their rights and responsibilities under the General Data Protection Regulations. This will be done by ensuring that all training identifies any data requirements within that subject area, and addresses this with attendees.

In addition, all new and existing employees will be required to undertake an e-learning course on the General Data Protection Regulations.

All policies have been reviewed to ensure that they are GDPR compliant and information has been placed in company offices and regional hubs to ensure that awareness of the importance of securing personal data is raised on a continuous basis.

MONITORING

The person responsible for monitoring the actions of the company in respect of data protection and for the content of all policies in respect of data protection will be the company Data Protection Officer. All actions in respect of data protection will be regularly reviewed with the Chief Executive Officer, the Chief Operating Officer and the Executive Team. Any amendments to this policy or the website statement will be agreed through the Executive Team.

New Policy: May 2018

Reason for Policy: To incorporate the General Data Protection Regulations (GDPR).

Reviewed: August 2018 – to incorporate internal organisational learning.

Next Review - May 2019