	Data Protection Policy
Date: March 2023	Date of Review: March 2025

Definitions:

Data Controller: exercise overall control over the purposes and means of the processing of personal data.

Data Processor: act on behalf of, and only on the instructions of, the relevant controller.

Personal data: information that relates to an identified or identifiable individual.

Further information on controllers, processors and personal information (links to ICO website).

EDNE is the Data Controller and holds various personal data in records about its employees and Board of Trustees to allow it to perform key tasks. EDNE also holds sensitive personal data about people who use our services.

EDNE adheres to the Data Protection Act 2018 including the following seven principles:

1. Lawfulness, fairness and transparency: You must have the right to process the data, it must not compromise the data subject, and everyone needs to be clear about what is being done.
2. Purpose Limitation: Why do you need to process personal data?
3. Data minimisation: Only process the data you need to.
4. Accuracy: Don't process data which is inaccurate.
5. Storage limitation: Only keep the data for as long as you need it.
6. Security: Keep the data safe.
7. Accountability: You are responsible for maintaining the privacy of personal data.

Introduction

Eating Distress North East (EDNE) is determined to ensure that its employees provide the best possible levels of service and act properly in accordance with EDNE's policies and procedures and according to relevant legislation.

This policy sets out the guidelines for the safeguarding of the movement of personal identifiable data in EDNE, and applies to all staff sessional workers, consultants volunteers, students and external workers.

Data security

All personal identifiable data will be collected, stored and used in accordance with this and EDNE's other relevant policies and procedures, i.e., Confidentiality, ICT Acceptable Use, and in accordance with the Data Protection Act 2018 and guidance within the Information Commissioner's Office Data Sharing Code of Practice.

EDNE's electronic data collection and storage system, Evide Impact Tracker is hosted on a secure server on Rackspace (ISO 27001 accredited) encrypted using 256 bit strong SSL encryption to maintain data privacy and integrity. The system is password protected and secure programming techniques are used to prevent unauthorised access. All data coming into the application is validated and filtered; all data out is escaped, and all forms are 'salted' to prevent CSRF attacks.

EDNE ensures the security of our data through the following security measures:

- All IT equipment and IT systems are password protected and passwords are changed every three months.
- No one other than EDNE employees and our processors can access our system.
- Personal data on our shared drive is separated into folders and permitted access is only granted to relevant staff members.
- Our processors only access our systems with the permission and knowledge of the person on the Service Level Agreement/contract.
- Our processors only access the data held on our systems when necessary to carry out the task required.
- Our processors are operating in a GDPR compliant environment and have confirmed this is the case.

All employees are responsible for ensuring that their passwords are secure and for not accessing or processing data in a manner which is contrary to this policy. EDNE employees should not, for example, send data to their personal email addresses or to any third parties or take personal data off site.

When using portable devices, for example laptops, tablets and phones, to access data EDNE employees and Board members should apply the same level of diligence when accessing from the office. Particular care should be taken when

using portable storage devices, for example USBs, and if any personal data is stored on the portable device EDNE employees and Board members should ensure it is encrypted. Password protection should be used for files as appropriate when remote working

Hard copy special category data (for example HR files) are stored in secured files in the office, the keys for which are stored in a secured key cupboard.

The EDNE office is locked when there is no one in the office.

Consent

The information EDNE holds contains both personal and special categories of data (sensitive personal data) as defined in guidance relating to the Data Protection Act 2018.

Consent to collect and store data will be obtained from service users at registration.

EDNE will make it clear to service users that data will be kept confidentially and safely in both manual and electronic safe havens, and that access to data is strictly controlled and that service users are made aware of their rights to view information kept about them. Circumstances in which disclosure may be required are made clear in EDNE service literature and will be done in ways that protect the user autonomy and respect their trust.

Individual's rights

EDNE upholds the following rights of the individual:

- 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 relation to automated decision making and profiling

EDNE upholds the right to see all personal notes and records under the Data Protection Act, if this includes a letter or additional information from another service, e.g. GP, then consent from this person will need to be obtained before the contents of the correspondence is disclosed.

Subject Access Requests

The UK Data Protection Act 2018 gives individuals (data subjects) power over their personal data including the right to access their data, have it corrected if wrong, and the right to have it deleted.

Individuals may not label their request (whether made by email, telephone or in person) a 'SAR' so it is imperative that all staff are familiar with the term, what constitutes a SAR and what to do if they receive one.

A SAR is when any individual asks what information EDNE holds on them, asks to see it and/or asks for it to be corrected or deleted.

Examples of a SAR include: asking their counsellor for a copy of their counselling records, asking the Office Manager for their HR/employment records or asking for all emails that EDNE holds relating to them.

What constitutes a valid SAR?

The Data Protection Act 2018 does not specify how to make a valid request. Therefore, an individual can make a request for rectification verbally or in writing.

SAR process

- We must reply within one month to a SAR and we cannot charge a fee, unless the request is "manifestly unfounded or excessive". That decision will be taken by the CEO and Counselling Lead.

  We can extend the time period if the request is complex but in these circumstances we must reply to the individual within one month to tell them the full response will take longer, and why.

- Upon receipt of a SAR, it needs to be forwarded to the CEO and Counselling Lead and documented in the SAR recording file (to ensure we record what date it was received).
- If the CEO / Counselling Lead are in the office forward the SAR to both and they will decide who is the most appropriate to deal with the SAR and record its receipt in the **SAR recording file**.
- If neither IAOs are in the office, forward it to them anyway but **you must document the SAR in the SAR recording file**.
- Upon receipt of a SAR, the CEO/Counselling Lead dealing with the request will compile the relevant personal data, send it to the data subject, and document the outcome in the **SAR recording file**.
- In some circumstances, for example if an ex-employee asks for their employment records, it may be necessary for EDNE to ask for further ID before responding to the SAR.

- Individuals have the right to request their personal data is deleted. However, there are some circumstances where this cannot be met, for example because we are legally obliged to keep the data (in the case of HR information).

- If an individual asks for their data to be deleted EDNE will decide if this request can be met and contact the individual to either comply (and explain consequences), or explain why the request cannot be met.

- If the SAR cannot be met the decision will be documented in the **SAR recording file**.

Responsibilities for data protection

EDNE has not appointed a single Data Protection Officer (DPO) for the following reasons:

- EDNE is not a public authority.
- Our core activities do not require large scale, regular and systematic monitoring of individuals.
- Our core activities do not consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

EDNE has given responsibility for information and data protection in the organisation to the CEO and Counselling Lead.

They are responsible for ensuring that:

- Anyone working for EDNE in any capacity is aware of this policy
- Any breaches of this policy coming to the attention of management are dealt with appropriately
- Monitoring of policy will take place in supervision and team meetings

All workers, volunteers, students or trustees are responsible for:

- Following this policy
- Ensuring that their collection, storage and use of data is confidential and secure, meets the professional standards of EDNE and complies with current legislation
- Being aware of circumstances in which disclosure may be required
- Reporting breaches as soon as they are suspected, or occur, to the Chief Officer
- Helping to keep this policy current and up-to-date

Data Retention and Disposal

Workers are encouraged to keep appropriate records of work with users which shall be accurate, respectful of users and colleagues and protected from unauthorised disclosure, taking into account their responsibilities and rights under data protection legislation and other legal requirements.

Therapists and counsellors are engaged in record-keeping for the following reasons:

- Relating to service delivery for purposes of management and administration, monitoring user progress and measuring outcomes
- To orient the therapist/counsellor towards user's key issues and relationships and identifying issues to take to supervision
- Professional development for reflection and /or accreditation purposes, and to contribute towards research
- For clinical records retention will be in accordance with BACP / BAAT guidelines
- For complaints and finance paperwork records will be retained for a minimum of seven years

Any breaches of this policy will be viewed as significant incidents and will be dealt with according to EDNE's disciplinary policies and procedures. Any training needs identified will be addressed by senior management.