DATA PROTECTION POLICY

Contents:

1: AIMS OF THIS POLICY

The Eggtooth Project needs to keep information on its staff, facilitators, therapists, volunteers, service users and any other stakeholders to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA 2018). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

2: DEFINITIONS

In line with the General Data Protection Regulation principles, The Eggtooth Project will ensure that personal and sensitive data will:

- be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- be obtained for a specific and lawful purpose
- be adequate, relevant but not excessive
- be accurate and kept up to date
- not to be held longer than necessary
- be processed in accordance with the rights of data subjects
- be subject to appropriate security measures described in section **8.**

N.B The definition of "Processing" is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data

as well as that kept on the computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all data it processes.

- **Accountability:** those handling personal data follow publicised data principles to safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the GDPR. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span in line with GDPR.

3: TYPES OF INFORMATION PROCESSED

The Eggtooth Project processes the following types of personal information:

Staff information – contact details, bank account number, id and employment information, supervision and feedback -

Volunteer information – contact details, id and employment information

Service user information – contact details, referral details and mental health history if appropriate and for some, detailed case notes may be held.

Personal information may be kept in the following forms:

- Paper based

- Computers based systems

4: RESPONSIBILITIES

DATA PROTECTION POLICY

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of The Eggtooth Project, this is the Board of Directors.

The Core Staff Team will support the Directors with the day to day management of this by maintaining and updating the required paperwork.

The Managing Director is responsible for:

- understanding and communicating obligations

- identifying potential problem areas or risks

- producing clear and effective procedures

All staff, facilitators, therapists and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principle.

5: POLICY IMPLEMENTATION

To meet our responsibilities, staff, facilitators, therapists and volunteers will:

- ensure any personal data is collected in a fair and lawful way

- explain why it is needed at the start

- ensure that only the minimum amount of information needed is collected and used

- ensure the information used is up-to-date and accurate

- review the length of time information is held

- ensure it is kept safely as described in section **8.**

- ensure the rights people have in relation to their personal data can be exercised.

We will ensure that:

- everyone managing and handling personal information is aware of this policy

- any disclosure of personal data will be in line with our procedures

- queries about handling personal information will be dealt with swiftly and politely.

6: AWARENESS

Staff, facilitators, therapists and volunteers will be reminded on a regular basis, through supervision and staff meetings, the importance of Data Protection.

DATA PROTECTION POLICY

7: GATHERING & CHECKING INFORMATION

Before information is collected, we will consider what details are actually required for the organisation's purposes and how long we are likely to require it for.

We will inform the people whose information is gathered about the following:

- why the information is being gathered

- what the information will be used for

- who will have access to the information (including any third parties).

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

If the information is required for another purpose, other than that originally stated when permission was first received, but even if the matter is related, consent will be required again in order to use the information.

8: DATA SECURITY

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- lockable cabinets and cupboards, with restricted access to keys

- password protection on personal and sensitive information

- computers set to restrict access to certain, sensitive areas

- where possible, personal data (paper hard copy, laptop) to be kept on site – in appropriate, secure storage when not in use.

- when personal data does need to be taken off site (whether paper hard copy or laptop) it must be kept safe and secure, preferably with the member of staff at all times. It must NOT be left in cars or anywhere that could be reasonably seen to be unsafe or unsecure

- laptops and memory sticks must be password protected

- data from computers is regularly backed up to cloud

Any unauthorised disclosure of personal data to a third party by staff may result in disciplinary proceedings .

9: DATA ACCESS REQUESTS

DATA PROTECTION POLICY

Anyone whose personal information we process has the right to know:

- what information we hold and process on them

- how to gain access to this information

- how to keep it up to date

- what we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

10: REVIEW

This policy will be reviewed at intervals to ensure it remains up to date and compliant with the law.

Policy status and review

Written by	**Franklyn Levey**
Review date (annual)	**18/12/24**