Eczema Outreach Support
DATA PROTECTION POLICY

1. Introduction

EOS holds different types of files containing personal data about staff, trustees, members and other contacts. In some instances, in particular relating to members and staff, sensitive personal data might also be held. This policy sets out how this data is handled in order to adhere to the principles set out in the General Data Protection Regulation (GDPR)

Article 4.1 of GDPR defines personal data as follows:
'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The GDPR further in article 9 imposes additional conditions for processing of sensitive personal data defined as
data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2. Responsibility for data protection

Due to the size of EOS there is no member of staff who can operate independently to oversee data protection, and there is therefore not a specific appointed Data Protection Officer.
Overall responsibility for data protection lies with the Board of Trustees.
Responsibility for implementation of this policy in day to day work lies with the CEO with input from the SMT.
All staff and trustees are responsible for adhering to the policy. Any breach of the policy could be a disciplinary offence.
Any queries on data protection should be directed to the CEO.

3. Categories of personal data

EOS holds several different types of personal data as set out below:

Members – contact details as well as information about children and sensitive personal data relating to health and family circumstances. For some members this could also include records of concern or child protection issues. It is also recorded when members donate money to EOS.
This information is primarily held in the CRM database. Some contact information can also be held in Office 365 and text messages are stored on EOS mobile phones. Limited information may also be held in online platforms, such as Eventbrite, but that would not be sensitive personal data.

Fundraisers/donors – contact details.
Information about fundraisers or donors who are not members is held online on Virgin Money Giving. This does not include any personal card payment details, which EOS cannot see. Donors who agree to further contact may also have their contact details and donation history logged in the CRM. EOS is also able to see who has raised funds forEOS via Facebook.

Staff – as well as contact details and work history, this also includes information on pay, pension, training, support & supervision records and any disciplinary action taken.
Any electronic files are held within the Office 365 Sharepoint SMT folder. Paper files are held in a locked cabinet in the EOS office.

Recruitment - contact details and work history details.
This information is stored in emails and within the Office 365 Sharepoint SMT folder.

Trustees – this includes contact details, CVs, signed codes of conducts and declarations of interests.
Electronic files are held within the Office 365 Sharepoint SMT folder. Paper files are held in a locked cabinet in the EOS office.

Professional contacts – contact details purely of a professional nature are held within the CRM database, Office 365 email files and on mobile phones.

4. Basis of holding information

Information on all members is held on the basis of consent through a privacy statement (appendix A), which is given when members register themselves or at the first contact with a member.

Details of fundraisers/donors who are not members are also held on the basis of consent.

Staff information is held on a contractual basis.

Recruitment information is gathered on the basis of legitimate interest and will only be used within the context of recruitment.

Information on trustees is legally required for reporting to OSCR (Office of the Scottish Charity Regulator).

Contact details held on people working with EOS in a professional capacity is gathered on the basis of legitimate interest as it is essential information for EOS to carry out its work and the data will only be used in the professional context of EOS's work.

5. Security

Details for storing personal data files are set out in the EOS document '*Data storage and disposal guidelines'*. (Appendix B)
A security assessment must be carried out at least every 12 months. (Appendix C)

It is the responsibility of all staff and trustees to keep information safe. Any breach of the guidelines can lead to disciplinary action.

6. Data Sharing

Data on individual members might be shared with healthcare professionals, schools and other statutory services if relevant for the member. The member will be made aware that sharing is happening, unless it is a child protection issue.
It is the responsibility of staff to make sure members are aware of data sharing.

EOS will never share any part of its member database with third parties. Third parties such as pharmaceutical companies may approach EOS for views from members. In such situations EOS will assess if the request is within EOS's charitable aims and if so EOS may distribute information or requests on behalf of the third party.

For specific projects it might be necessary to give an IT company access to the EOS members database. In such circumstances a specific agreement must be made between EOS and the IT company to ensure the data is kept safe and not shared in any form with third parties.

Parts of staff files are shared with the payroll provider and the pension provider.

7. Data retention

EOS has a data retention schedule (Appendix D) detailing how long documents are kept for.

8. Data access requests

All data subjects (members, staff, trustees etc) have the right to request a record of the information EOS holds on them. Any such request should be directed to the CEO in the first instance, who might then delegate to a member of staff.

9. Data Breach

Any member of staff or trustee becoming aware of a potential data breach must inform the CEO immediately.