EYPCF – East Yorkshire Parent Carer Forum - Data Protection Policy

Registered charity no.117499

1. Legal Duty

The Charity has a legal responsibility to ensure all information is processed in accordance with the Data Protection Acts 1998 2003 2017 (General Data Protection Regulations - GDPR).
The Data Protection Acts (the Acts) aim to protect all personal data which is collected, processed, stored and disposed of by an organisation. Personal data is information about a living, identifiable person.
The Acts apply to data in paper and electronic format including images
This policy applies to all our employees, Trustees, steering group members and volunteers.
This policy covers the homes, offices and computers/phones of Trustees and steering group members if used for EYPCF business, the EYPCF offices, all venues used by EYPCF.

1.2 Data Protection Principles

The Acts identify eight principles which the Charity, and those working within it, MUST legally comply with. Additionally the Charity is not required to register with the Information Commissioners Office (ICO) to allow data storage, handling etc.:-

1. Personal Data shall be processed fairly and lawfully

2. Processing Personal Data for specified purposes

Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or other purpose

3. Information Standards – the amount of Personal Data you may hold

Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4. Information Standards – keeping Personal Data accurate and up to date

Personal Data shall be accurate and, where necessary, kept up to date

5. Information Standards – retaining Personal Data

Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purposes or those purposes

6. The Rights of Individuals

Personal Data shall be processed in accordance with the rights of data subjects under this Act.

7. Information Security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and accidental loss or destruction of, or damage to,

Personal Data. In practice it means that the Charity will have appropriate security to prevent the Personal Data held being accidentally or deliberately compromised.

8. Sending Personal Data outside the European Economic Area (EEA)

Personal Data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures adequate protection of the rights and freedoms of data subjects in relation to the processing of Personal Data.

2 Definitions

Confidentiality: Confidential information is defined as verbal or written information, which is not meant for public (this may include our partners in health and local authority) or general knowledge, information that is regarded as personal by users, members, trustees, employees or volunteers

Consent: of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by a statement or clear affirmative action, signifies agreement to the processing of personal data related to him or her.

Data is one piece or a combination of information that relates to a person or a 'Data Subject' that could identify them, that is stored:

a) Electronically i.e. on computer, including word processing documents, emails, computer records, CCTV images, microfilmed documents, backed up files or databases, faxes and information recorded on telephone logging systems.

b) Manually i.e. records which are structured, accessible and form part of a filing system where individuals can be identified and personal data easily accessed without the need to trawl through a file.

Data Controller or Controllor : The person who (either alone or with others) decides what personal information we will hold and how it will be held or used. In this case the trustees.

Data Processor or Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. Currently the administrator.

Data Protection Act 1998: The UK legislation that provides a framework for responsible behaviour by those using personal information, which will be superseded by the General Data Protection Regulations on 25 May 2018.

Data Subject: any living individual whose personal data is being processed. Examples include:

- employees – current and past
- volunteers
- job applicants
- donors
- service users/clients
- suppliers

'Explicit' consent: is a freely given, specific and informed agreement by an individual to the processing of personal information about them, leaving nothing implied. Explicit consent is needed for processing sensitive data.

Information Commissioner is responsible for implementing and overseeing the General Data Protection Regulations

Notification is notifying the Information Commissioner of the data processing activities of EYPCF. The EYPCF is subject to an exemption.

Personal data breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Processing: means the use made of personal data including any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Data Protection Adviser: The person(s) responsible for ensuring that we follow our data protection policy and complies with the General Data Protection Regulations and is the central point of contact for subject access requests.
Sensitive Data – Factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person
Third Party agreements. Many organisations use third parties to store/process data such as: online payments, online forums, cloud storage facilities. There should be a third party written agreement with the other organisation to confirm they are meeting the regulations. These can sometimes be found as web based documents. The data needs to be stored on European servers to ensure they comply with GDPR

3 Policy Statement

It is necessary for EYPCF to keep records of personal details of parent carers and other individuals, their circumstances and of EYPCF contact with them. This recordkeeping serves many purposes, including facilitating the smooth running of EYPCF, enabling it to maximise the help it gives to individuals and for monitoring purposes.

This personal information must be collected and dealt with appropriately– whether on paper, in a computer, or recorded on other material. This policy applies to all personal and sensitive personal data. We will:

- comply with the General Data Protection Regulations in respect of the data we hold about individuals;
- respect individuals' rights;
- be open and honest with individuals whose data is held;
- ensure that everyone processing personal information understands that they are all responsible for following good data protection practice;
- protect the organisations members, employees, volunteers and other individuals;
- provide training, support and supervision for employees and volunteers who handle personal data, so that they can act legally, confidently and consistently;
- regularly assess and evaluate our methods and performance in relation to handling personal information; and
- protect the organisation from the consequences of a breach of its responsibilities.

We recognise that our first priority under the General Data Protection Regulations is to avoid causing harm to individuals. Information about employees, volunteers and members will be used fairly, securely and will not be disclosed to any person unlawfully.

Secondly, the Regulations aim to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, we will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

3.1 Data Controller

Trustees of EYPCF are the Data Controller under the Act, which means that they determines what purposes personal information held, will be used for.

3.2 Disclosure

We do not normally share personal data with any other agencies. Anonymised data may be shared with our partners eg : local authority, health in order to support the identification of gaps in service provision and development of new services.

There are circumstances where the law allows us as an organisation to disclose data (including sensitive data) without the data subject's consent. These are requests from law enforcement agencies and for national security. However before any data is processed steps will be taken to ensure the request is legitimate and approval sought by the Data Advisers from the Trustees.

4 Responsibilities

The Trustees recognises their overall responsibility for ensuring that EYPCF complies with its legal obligations.
The Data Protection Advisers are currently **Shirley Pethick and Sheena Withers** who have the following responsibilities:

- Briefing the Trustees and steering group committee on Data Protection responsibilities;
- Reviewing Data Protection and related policies in line with agreed schedule;
- Advising other staff, trustees, steering group members and volunteers on Data Protection issues;
- Ensuring that Data Protection induction and training takes place;
- Handling Data subject access requests;
- Approving unusual or controversial disclosures of personal data;
- Checking and approving any contracts or agreements with third parties that may handle sensitive data

- Electronic security;

- Ensuring that all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been disposed of or passed on/sold to a third party.

- Approving data protection-related statements on publicity materials and letters

Each employee, trustee, steering group member and volunteer who handles personal data will comply with the organisation's policy for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed. All employees, trustees, steering group members and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy and breach of personal data may result in removal from the board of trustees or the steering group.

5. Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, we have a separate Confidentiality Policy. This Data Protection Policy should be read in conjunction with the Confidentiality Policy.

Where anyone within our organisation feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done after discussions with the Data Advisers and with the minuted approval of the Trustees. All such disclosures will be documented

6. Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Any recorded information on members, volunteers and employees will be:

• Handled, transferred, processed and stored with the utmost care and regard.
• When not being handled, transferred or processed, it will be stored in secure office facilities, locked drawers or cabinets.
• Protected by the use of passwords if kept on computers and/or other devices and encrypted if appropriate.
• Destroyed confidentially if it is no longer needed, or if an individual requests.

- Trustees and steering group members are required to store the minimum amount of data on their home devices including emails. Advise can be obtained from the data adviser.

Remember this policy applies to home offices and computers/phones if used for EYPCF business as well as EYPCF office and venues.

Access to information on the main database is controlled by a password and only those needing access are given the password. Employees, Trustees, steering group members and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display. The same applies to any paper copies out on desks.
Notes regarding personal data of clients should be shredded or destroyed.

7. Data Recording and storage

We have a single database for holding basic information about all members and volunteers. Back ups are taken frequently and are tested regularly. The back-up copies of data are kept in a safe place.
We will regularly review our procedures for ensuring that our records remain accurate and consistent and, in particular:

- We will keep records of how and when information was collected.
- The storage system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- All employees, Trustees, steering group members and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Effective procedures are also in place to address requests from Data Subjects for access to, amendments or the erasure of their information
- Data will be corrected if shown to be inaccurate or a request is made by a Data Subject.

We store archived paper records of members and volunteers securely in the office. Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

7.1 Web site and facebook

The EYPCF website contains links to other websites. These third party sites have separate and independent privacy policies. EYPCF therefore has no responsibility or liability for the content and activities of these linked sites.

Comments posted on the EYPCF Facebook account must be approved by EYPCF prior to publication. EYPCF reserves the right to take action regarding comments which are deemed to contain inappropriate language, false accusations or personal attacks. Action may range from simply deleting a comment and providing a warning, up to and including banning a user from future commenting privileges. Users are strongly advised not to disclose personal information over the Internet, and to keep their usernames and passwords secure at all times.

8. **Access** to Data

Information and records will be stored securely and will only be accessible to authorised employees and volunteers, and the individual to whom the information relates.

All members and volunteers have the right to request access to all information stored about them. Any subject access requests will be handled by the Data Protection Adviser within the required time limit.

Subject access requests must be in writing or by email. All employees, Trustees, steering group members and volunteers are required to pass on anything which might be a subject access request to the Data Protection Adviser without delay. In accordance with the GDPR, we will provide personal data in a 'commonly used and machine readable format.' We also recognise the right of the individual to transfer this information to another Controller.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.
The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

EYPCF may withhold access in certain circumstances including:

- where the data has originated from a third party
- where the data was provided explicitly on a confidential basis by a third party acting in a professional capacity (such as a doctor or social worker).
- where the data contains information that relates to an identifiable third party

In any case where a file contains information about more than one person, great care will be taken when providing an individual with access to his/her personal data to avoid inadvertently breaching the confidentiality of a third party.

9. Data breach reporting

All Staff, Trustees, steering group members and volunteers are required to report any data breach to the Data Protection Adviser as soon as possible once they are aware it has occurred. A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to data transmitted stored or otherwise processed.

The Data Controller is responsible for recording or reporting any data breachs.

Less serious breaches will be recorded and listed in an appropriate place, and trends or lessons learned will be reviewed.

Serious personal data breaches will be reported by the Data Protection Adviser to the Trustees at the earliest possible time, as well as reported to the ICO within 72 hours of the breach occurring if possible, and if not, informing the ICO the reason for the delay.

10. Transparency

We are committed to ensuring that in principle Data Subjects are aware that their data is being processed and:

- for what purpose it is being processed;
- what types of disclosure are likely; and
- how to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

By accessing the Data protection policy
By reading the privacy notice on the web site

11. Consent

Information about volunteers, members of steering group will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role. Consent will be sought for the use of any images.

Information about members will only be made public with their explicit consent. (This includes photographs.)
Consent will be obtained from parents, if children's data is being stored or processed depending on the age of the child/young person in accordance with legislation.

Consent should be given in writing, although for some services it is not always practicable to do so. In these cases verbal consent will always be sought to the storing and processing of data, and records kept of the dates, and circumstances. Online consent will be requested when clients sign up to services, donate or sign up to mailing lists. In all cases it will be documented on the database that consent has been given.

All Data Subjects will be given the opportunity to opt out of their data being used in particular ways. We do not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.

We acknowledge that, once given, consent can be withdrawn by the Data Subject at any time. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

13. Volunteer training and acceptance of responsibilities

All volunteers, trustees and members of the steering group will be given copies of all relevant policies and procedures during their induction process, including the Data Protection policy and

Confidentiality Policy. All trustees, steering group members and volunteers will be expected to adhere to all these policies and procedures. A signed copy of the policy confirms that it has been read and understood and will be adhered too. Any queries should be addressed to the Data Protection Advisers.

Data Protection will be included in trustee training and the induction training for all steering group members and volunteers.

We will provide opportunities for all staff, trustees, steering group members and volunteers as appropriate to explore Data Protection issues through training, team meetings, and supervisions.

14. Policy review

This policy will be reviewed and updated as necessary in response to changes in relevant legislation, contractual arrangements, and good practice or in response to an identified failing in its effectiveness.

In case of any queries in relation to this policy please contact our Data Protection Advisers Shirley Pethick or Sheena Wither at
Unit 21,
Bridlington Business Centre,
Enterprise Way
Bridlington
YO16 4SF

www.eypcf.co.uk

Trustees approved date……

Review date Oct 2020