East Durham PARTNERSHIP
Supporting Communities

Policy on

Data Protection

East Durham Partnership is committed to safeguarding & promoting the welfare of children and young people, as well as vulnerable adults, and expects all staff and volunteers to share this commitment.

East Durham Partnership

Data Protection Policy

(Equality and Diversity Assessment)

We will consider any request for this procedure to be made available in an alternative format.

We review our policies and procedures regularly to update them and to ensure that they are accessible and fair to all. All policies and procedures are subject to equality impact assessments. Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a different impact on grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation or human rights.

We are always keen to hear from anyone who wants to contribute to these impact assessments and we welcome suggestions for improving the accessibility or fairness of the policy.

Equality Impact Assessed: May 2018

East Durham Partnership

Data Protection Policy

1. Scope

This Policy will enable compliance with relevant Data Protection Legislation and will be relevant to all staff and outsourced service providers operating under data processing contracts or agreements with East Durham Partnership. East Durham Partnership is registered, with Information Commissioners Office under the following:

- Organisation name: **EAST DURHAM PARTNERSHIP LTD**
- Registration reference: **Z1410663**

This Policy applies to all the information East Durham Partnership holds in any format. Definitions of terms and the designation of articles referenced in this policy should be obtained from the GDPR Articles published by the EU[1].

This Policy will form part of the East Durham Partnership 'record of processing activities'.

2. Role definitions

East Durham Partnership is the Data Controller for all personal data held in its systems

The Data Protection Officer (DPO) for East Durham Partnership is the Senior Compliance Officer, (email: DPO@eastdurhampartnership.co.uk)

A Data Owner is the person who holds managerial and financial accountability for a data set and determines its purposes and means of processing.

3. Responsibilities

The Trustees of East Durham Partnership is responsible for ensuring that East Durham Partnership has a Data Protection Policy.

The Data Protection Officer is responsible for :

- authorising and requiring action in relation to data protection processes and procedures, risk and privacy assessments
- resourcing of staff training

[1] See https://gdpr-info.eu/

- keeping the register of processing activities and inform, advise and recommend in relation to data protection;

- have due regard for the risks associated with processing personal data.

In addition the Data Protection Officer will:

- be easily accessible, with all staff made aware of the role;
- have the necessary level of expert knowledge;
- have sound knowledge of East Durham Partnership rules and procedures;
- not hold a position where she or he determines the purposes or means of processing personal data;
- foster a data protection culture and implement essential elements of the law;
- be involved in all issues relating to the protection of personal data;
- be consulted on any data breach incident;
- given the resources and training necessary to fulfil DPO duties;
- act independently and not be instructed or influenced;
- not be penalised for performing tasks required by the role as set out in the legislation and working party guidance.

Data Owners are responsible for the processing (ie. the collection, use, storage and retention) of personal data are responsible for ensuring their processing is done in compliance with this policy and the law.

All staff are responsible for familiarising themselves with this policy and complying with a request for information from DPO.

Compliance with this Policy is compulsory for all staff employed by East Durham Partnership. A member of staff who fails to comply with the Policy may be subjected to action under the organisations disciplinary policy.

4. Relationship with existing policies and legislation

This policy will facilitate compliance with the following legislation and guidance:

- General Data Protection Regulation[2]
- Data Protection Act 1998 (and any successor legislation)
- Crime and Justice Directive
- Privacy and Electronics Communications Regulations 2003
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Article 29 Working Party Guidance

[2] References to 'articles' throughout will refer to the text of the GDPR as published by the EU

This Policy has been formulated within the context of the following GDPR guidance notes :.

- Guidance Note 1: Making a DP Request
- Guidance Note 2: Data Protection for Staff
- Guidance Note 3: Providing References
- Guidance Note 4: Code of Conduct for Photographs and Recordings
- Guidance Note 5: Use of Online Survey Software
- Guidance Note 6: Conducting a Privacy Impact Assessment
- Guidance Note 7: Creating Privacy Notices

5. Data Protection Principles

a. *Lawfulness, fairness and transparency*

To ensure that personal data is processed lawfully, the organisation will not process personal data unless one of the conditions of processing in article 6 is met or article 9 where relevant to the processing of sensitive personal data.

Where consent is used as the condition for processing then the conditions in article 7 and 8 will be met.

b. *Purpose limitation*

East Durham Partnership will ensure that all processing of personal data is undertaken for specific, explicit and legitimate purposes and that the data is not further processed in a manner that is incompatible with those purposes.

c. *Data minimisation*

East Durham Partnership will ensure that personal data processed is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d. *Accuracy*

East Durham Partnership will ensure there are mechanisms to ensure personal data remains accurate and up to date.

e. *Storage limitation*

East Durham Partnership will ensure that personal data is retained no longer than necessary.

f. *Integrity and confidentiality*

East Durham Partnership will ensure that personal data is processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing, accidental loss, destruction or damage using appropriate technical measures.

6. Data Subject Rights

a. *Information and Access*

East Durham Partnership will ensure all communications in relation to processing are done in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Requests for access to personal data in relation to data subject rights will be managed by the DPO.

Requests for access to personal data in relation to data sharing arrangements will be managed by the member of staff named in the agreement.

b. *Rectification and erasure*

East Durham Partnership recognises the right of users to request rectification and erasure of their data in specific circumstances according to legislation.

Routine requests for amendments to personal data will be managed by the department responsible for processing the data.

Non-routine requests for rectification and erasure in relation to personal data will be identified by the department processing the data and referred to the DPO, all requests will be managed with due regard for Articles 16-19 of the GDPR.

c. *Objection and restriction*

East Durham Partnership recognises the rights of users to object to processing and to ask us to restrict our processing activities.

d. *Portability*

Where East Durham Partnership already holds data in machine readable format a requester may request a copy in the same format.

e. Automated processing

East Durham Partnership does not carry out automated processing as a matter of course. If a data subject is to be subject to automated processing as a result of participation in an ad-hoc project then they will be informed as part of the Privacy Notice for that project about the nature of the processing and their rights in relation to it.

7. Controller / Processor Responsibilities

Where data is held externally or 'hosted' by a third party, the third party is deemed to be a 'processor' and the requisite contractual obligation should be placed upon them unless they have already undertaken equivalent obligations in their standard terms and conditions.

This obligation will be to comply fully with the requirements of this policy and fulfil its duties under law regarding the security and integrity of the data supplied by East Durham Partnership

8. Data Sharing Agreements

Data sharing between a Controller and Processor should be covered by a contract. This contract may be part of the terms and conditions of purchase in relation to hosted data services but will always need to define the Controller/Processor relationship.

Data sharing between two Controllers should be covered by a Data Sharing Agreement.

A Data Sharing Agreement may be a schedule included as part of a contract or a separate document. It will describe the process for sharing data, including the legal basis for the sharing and processing.

In cases where a third party organisation needs access to East Durham Partnership system containing personal data an agreement will be put in place.

The Data Protection Officer will maintain a list of relevant agreements and contract clauses.

9. Data Breaches

Data breach incidents will be reported to the Data Protection Officer

The Data Protection Officer will log the breaches and issue recommendations taking into account mitigation already applied In line with legislation, the recommendations should be acted upon within 72 hours of the breach being reported.

Where the Data Protection Officer recommends that the breach is reportable to the Information Commissioner, the Trustees must be informed.

10. Privacy Impact Assessments

Where a new system is implemented in which personal data will be processed, a Privacy Impact Assessment must take place. A Privacy Impact Assessment should be conducted by the Data Owner for the personal data concerned.

Privacy Impact Assessments must be reviewed by the Data Protection Officer. This should be done as part of the implementation plan for a new system.

11. Evaluation and review

The performance of this Policy will be reported on annually and it will be formally reviewed every five years by the Trustees

In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

Implementation Date: **May 22nd 2018**
First Review Date: **May 2023**