

ECDP Data Management Policy

1. Contents

Introduction	1
Our Commitment to Data Protection	2
Definitions	2
Personnel	3
The Individual / Data Subject	3
Collecting and Processing Personal Data	5
Data Retention	5
Data Storage and Security	6
Sharing Data	7
Key Contacts	7
Policy Change Record	8

2. Introduction

The policy and guidelines set out in this document apply to Trustees, employees, freelancers, contractors and volunteers of Essex Cultural Diversity Project (ECDP). It also applies to our contracts with third party suppliers who process data on our behalf.

It is informed by the UK GDPR and the Data Protection Act 2018 (DPA), which implements the EU General Data Protection Regulation (GDPR). These regulate the processing of information relating to living individuals, including the obtaining, holding, processing or disclosure of such information. They outline obligations on the part of an organisation to keep such information secure. They also include the right of individuals to see personal information held about them by an organisation, and the right to challenge the accuracy of data held. Failure to comply and serious infringements of the DPA may result in heavy financial penalties.

More information about the Data Protection Act 2018: <https://www.gov.uk/government/collections/data-protection-act-2018>

More information about the UK GDPR and Data Protection: <https://ico.org.uk/>

This core policy outlines how ECDP handles or processes data. Our Privacy Statement is a separate document, which references this document, that explains ECDP's information practices and the choices

individuals can make about how information about them is collected online and used by ECDP.
<https://essexcdp.com/privacy>

3. Our Commitment to Data Protection

- 3.1. ECDP committed to ensuring its Trustees, staff, freelancers, contractors, volunteers and any authorised third parties carry out these activities in accordance with current UK data protection law as it recognises that the correct and lawful treatment of this data will maintain confidence in ECDP and will provide for successful operations.
- 3.2. In accordance with the principles of the Data Protection Act 2018 (DPA), which implements the EU General Data Protection Regulation (GDPR), ECDP will ensure that all personal data that it holds will be:
 - i) processed lawfully, fairly and in a transparent manner;
 - ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - iii) adequate, relevant and limited to what is necessary;
 - iv) accurate and kept up to date;
 - v) kept in a form which permits identification of data subjects for no longer than is necessary;
 - vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- 3.3. ECDP's Privacy Statement is published online to explain ECDP's information practices and the choices individuals can make about how information about them is collected online and used by ECDP. <https://essexcdp.com/privacy>

4. Definitions

- 4.1. **Data Subject:** a data subject is an identifiable individual person about whom the ECDP holds personal data.
- 4.2. **Personal Data:** any information relating to an identifiable living person who can be directly or indirectly identified, for example from a name, identification number, location data or online identifier.
- 4.3. **Personal Data breach:** the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- 4.4. **Processing:** anything that can be done with Personal Aata, including 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.

5. Personnel

- 5.1. **Data Controller:** person(s) or an authority which determines the purposes and means of the processing of personal data. In the case of ECDP, the Data Controller is Essex Cultural Diversity Project Ltd
- 5.2. **Data Processor:** a person or authority which processes personal data on behalf of the controller. In the case of ECDP the Data Processors are Indi Sandhu, Creative Director and CEO for ECDP, and Jo Nancarrow, Admin and Digital Lead (Freelance).
- 5.3. **Data Protection Officer:** Usually a person or authority in an independent role who ensures compliance with data protection law. In the considered opinion of the Trustees the scope and nature of the personal data held by ECDP is not sufficient to warrant the appointment of a Data Protection Officer. Accordingly, no Data Protection Officer is appointed.

6. The Individual / Data Subject

6.1. Rights of the Data Subject:

In compliance with The Data Protection Act 2018 (DPA), which implements the EU General Data Protection Regulation (GDPR), ECDP will give data subjects the following rights. These rights will be made clear in the Privacy Statement provided to data subjects:

6.1.1. RIGHT TO BE INFORMED

Individuals should be informed of how their data is collected, stored and processed in a clear, accessible way. When collecting personal information ECDP will provide to the data subject free of charge, a Privacy Statement written in clear and plain language which is concise, transparent, intelligible and easily accessible containing the following information:

- (i) Identity and contact details of the controller
- (ii) Purpose of the processing and the lawful basis for the processing
- (iii) The legitimate interests of the controller or third party, where applicable
- (iv) Details of transfers to third country and safeguards
- (v) Retention period or criteria used to determine the retention period
- (vi) The existence of each of data subject's rights
- (vii) The right to withdraw consent at any time, where relevant
- (viii) The right to lodge a complaint with a supervisory authority

6.1.2. RIGHT OF ACCESS

Individuals can request access to a copy of their data in electronic form and details of how it is processed.

6.1.3. RIGHT TO RECTIFICATION

Individuals are entitled to have their data corrected if it is inaccurate or incomplete.

6.1.4. RIGHT TO ERASURE

Also known as 'the right to be forgotten', this permits individuals to request the deletion of their data. Except where the data are held for purposes of legal obligation or public task.

6.1.5. RIGHT TO RESTRICT PROCESSING

Where there is a dispute between the data subject and the Controller about the accuracy, validity or legality of data held by ECDP the data subject shall have the right to require the Controller to cease processing the data for a reasonable period of time to allow the dispute to be resolved.

6.1.6. RIGHT TO DATA PORTABILITY

Where data is held for purposes of consent or contract the data subject shall have the right to require the controller to provide him/her with a copy in a structured, commonly used and machine-readable format of the data which he/she has provided to the controller, and have the right to transmit those data to another controller without hindrance.

6.1.7. RIGHT TO OBJECT

a) The data subject shall have the right to object, on grounds relating to his/her/their particular situation, at any time to processing of personal data concerning him/her/them which is based Public Task or Legitimate Interest (4.5 or 4.6), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

b) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him/her/them for such marketing, which includes profiling to the extent that it is related to such direct marketing.

c) Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

d) At the latest at the time of the first communication with the data subject, the right referred to in paragraphs a) and d) shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

6.2. Right of Access, Rectification and Erasure:

Data subjects will be clearly informed of their right to access their personal data and to request that any errors or omissions be corrected promptly. Such access shall be given and the correction of errors or omissions shall be made free of charge provided that such requests are reasonable and not trivial or vexatious. There is no prescribed format for making such requests provided that:

a) the request is made in writing, signed & dated by the data subject (or their legal representative);

b) the data claimed to be in error or missing are clearly and unambiguously identified;

- c) the corrected or added data are clear and declared by the subject to be complete and accurate.

It will be explained to subjects who make a request to access their data and/or to have errors or omissions corrected, or that their data be erased, that, while their requests will be actioned as soon as is practical there may be delays where the appropriate volunteers or staff to deal with the request do not work on every normal weekday.

Where a data subject requests that their data be rectified or erased the Data Controller and Data Processor will ensure that the rectifications or erasure will be applied to all copies of the subject's personal data including those copies which are in the hands of a Third Party for authorised data processing.

6.3. Right of Portability

ECDP will only provide copies of personal data to the subject (or the subject's legal representative) on written request. ECDP reserves the right either:

- a) to decline requests for portable copies of the subject's personal data when such requests are unreasonable (i.e.: excessively frequent) or vexatious;

or

- b) to make a reasonable charge for providing the copy.

7. Collecting and Processing Personal Data

- 7.1. Personal data must only be collected and processed for clearly specified purposes, and must have a valid lawful basis (such as with the Data Subject's consent, by contract or by legal obligation).
- 7.2. All forms requesting personal data, whether in electronic or paper format, must contain information on who is collecting the data (normally "Essex Cultural Diversity Project (ECDP)"); an explanation of the purpose(s) for which the data is being collected; a link to ECDP's Privacy Statement.
- 7.3. All forms requesting personal data, whether in electronic or paper format should use clear and plain language and be easily accessible and easy to understand.
- 7.4. When asking for consent to collect and hold Personal Data for uses such as email marketing and mailing lists, the Data Subject must always be given the choice to opt-in.
- 7.5. Information that has been obtained on the basis of consent should always be maintained with a record of when consent for data processing has been obtained; the nature of processing that has been consented to; who entered the data.

8. Data Retention

Personal data shall not be retained for longer than:

- a) In the case of data held by subject consent:
the period for which the subject consented to ECDP holding their data

- b) in the case of data held by legitimate interest of ECDP:
the period for which that legitimate interest applies. For example: in the case of data subjects who held a role, such as a contracted Freelancer, the retention period is that for which ECDP reasonably has a legitimate interest in being able to identify that individual's role in the event of any retrospective query about it, which should be no longer than two years after end of the contract or role
- c) in the case of data held by legal obligation:
the period for which ECDP is legally obliged to retain the data.

ECDP shall regularly – not less than every 6 months – review the personal data which it holds and remove any data where retention is no longer justified. Such removal shall be made as soon as is reasonably practical, and in any case no longer than 20 working days (of the relevant Data Processor) after retention of the data was identified as no longer justified.

9. Data Storage and Security

- 9.1. **Anonymisation:** When a person's identification is not needed or relevant to the processing of the data, data will be anonymised.
- 9.2. **Storage:** Data Processors will ensure that Personal Data will be kept secure at all times, whether it is in hard copy or electronic format, on or offline. For offline storage of electronic personal data ECDP will purchase and own at least 2 and not more than 5 removable storage devices to store the personal data that it holds and processes. When not in use the removable storage devices will be kept in a secure location and reasonably protected against accidental damage, loss, avoidable theft or other misuse by persons other than the Data Processors. The Data Controller will keep a register of the location of all removable devices used for the storage and processing of personal data.
- 9.3. **Backup:** The removable storage devices will also act as backup devices. To protect against loss of data by accidental corruption of the data or malfunction of a removable data storage device (including by physical damage), all ECDP's personal data shall be backed up periodically and whenever any significant changes (additions, amendments, deletions) are made to the data. Backup copies of the data shall be held in separate secure locations which are not susceptible to common risks (eg: fire, flood, theft).
- 9.4. **Data Processing Location:** Data Processors shall only process Personal Data related to ECDP and its activity in a secure location, and not in any public place where Personal Data could be overlooked by others, or the removable data storage devices would be susceptible to loss or theft.
- 9.5. **Obsolete or Dysfunctional Equipment:** Equipment used to hold personal data, whether permanently or as interim working copies, which come to the end of their useful working life, or become dysfunctional, shall be disposed of in a manner which ensures that any residual personal data held on the equipment cannot be recovered by unauthorised persons.
- 9.6. **In the event of a Data Breach:** Any loss of personal data, or breach of data security must be reported immediately to ECDP Trustees' named Data Controller(s), without delay after first becoming aware of any data breach. The Data Controller(s) must report serious personal data breaches to the Information Commissioner within 72 hours. Data processors who are handling data are required to notify ECDP. In the event that full details of the nature and consequences of the data breach are not immediately accessible (for example because Data Processors do not

work on every weekday) the Trustees will bring that to the attention of the Information Commissioner's Office and undertake to forward the relevant information as soon as it becomes available.

10. Sharing Data

- 10.1. Under no circumstance will ECDP share with, sell or otherwise make available to Third Parties any personal data, except where it is necessary and unavoidable to do so in pursuit of its charitable objects as authorised by the Data Controller, or if it has a data sharing agreement with another organisation as part of a joint project
- 10.2. In the rare circumstances where personal data is shared with a partner organisation or Third Party, Data Subjects will be informed in advance of or at the time of data collection and/or consent.
- 10.3. If sharing personal data with a Third Party, a Data Sharing Agreement will be signed by ECDP and the Third Party which stipulates that:
 - a) ECDP is the owner of the data
 - b) The Third Party will hold and process all data shared with it exclusively as specified by the instructions of the Data Controller
 - c) The Third Party will not use the data for its own purposes, outside of the uses consented to by the Data Subject
 - d) The Third Party will ensure that the data is held securely and protected from theft, corruption or loss
 - e) The Third Party will be responsible for the consequences of any theft, breach, corruption or loss of ECDP's data (including any fines or other penalties imposed by the Information Commissioner's Office) unless such theft, breach, corruption or loss was a direct and unavoidable consequence of the Third Party complying with the data processing instructions of the Data Controller
 - f) The Third Party will not share the data, or the results of any analysis or other processing of the data with any other party without the explicit written permission of the Data Controller
 - g) The Third Party will securely delete all data that it holds on behalf of ECDP once the purpose of processing the data has been accomplished
 - h) The Third Party will not transfer personal data out of the UK.

11. Key Contacts

ECDP Trustee contact for this policy:

Jo Webb, jowebb@essex.ac.uk

Data Processors:

Indi Sandhu | ECDP's Creative Director and CEO
indi.sandhu@essexcdp.com | 07863 203732

Jo Nancarrow, ECDP's Admin and Digital Lead (Freelance)
jo@essexcdp.com | 07952563451

Information Commission's Office: 0303 123 1113 / <https://ico.org.uk>

For a guide to the GDPR, data processing and protection, and to report any data breaches

12. Policy Change Record

Date of Change:	Changed By:	Comments:
03/2022	JN	Drafted Discussed with key members in Core Team and Trustees
05/2022	JN	Policy approved by ECDP Trustees at ECDP AGM Posted online at https://essexcdp.com/data-management-policy/