Data Protection Policy

Overview of the General Data Protection Regulation

Creative Futures will ensure that all personal data that it holds will be:

- ☑ processed lawfully, fairly and in a transparent manner;
- ☑ collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- ☑ adequate, relevant and limited to what is necessary;
- ☑ accurate and kept up to date;
- ☑ kept in a form which permits identification of data subjects for no longer than is necessary;
- ☑ 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.

Contents (Summary)

Full Contents

Data Protection Policy

1. Introduction to the GDPR

Under the EU General Data Protection Regulations (GDPR) Creative Futures (UK) Limited (herein after referred to as "the Charity") is required to comply with the GDPR and undertakes to do so.

Throughout this policy document, numbers prefixed by "Art:" in brackets *(eg: {Art:5})* refer to the relevant Article(s) in the GDPR.
Extracts of relevant GDPR Articles are contained in an Appendix, available separately.

2. Definitions *{Art:4}*

The definitions of terms used in this policy are the same as the definitions of those terms detailed in Article-4 of the GDPR.

Data Subject

A data subject is an identifiable individual person about whom the Charity holds personal data.

Contact Information

For the purposes of this Policy, "Contact Information" means any or all of the person's:
full name (including any preferences about how they like to be called);
full postal address;
telephone and/or mobile number(s);
e-mail address(es);
social media IDs/UserNames (*eg:* Facebook, Skype, Hangouts, WhatsApp)

3. Principles of the GDPR *{Art:5}*

The Charity will ensure that all personal data that it holds will be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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, using appropriate technical or organisational measures.

4. Lawful Processing

The Charity will obtain, hold and process all personal data in accordance with the GDPR for the following lawful purposes.

In all cases the information collected, held and processed will include Contact Information (as defined in 2 above).

4.1 By Consent

a) People who are interested in, and wish to be kept informed of, the activities of the Charity.

b) Subject to the person's consent, this may include information selected and forwarded by the Charity on activities relevant to those of the Charity by other organisations.
Note: this will not involve providing the person's personal data to another organisation.

The information collected may additionally contain details of any particular areas of interest about which the person wishes to be kept informed.

The information provided will be held and processed solely for the purpose of providing the information requested by the person.

4.2 By Contract

People who sell goods and/or services to, and/or purchase goods and/or services from the Charity.

The information collected will additionally contain details of:

a) The goods/services being sold to, or purchased from the Charity;

b) Bank and other details necessary and relevant to the making or receiving of payments for the goods/services being sold to, or purchased from the Charity.

The information provided will be held and processed solely for the purpose of managing the contract between the Charity and the person for the supply or purchase of goods/services.

4.3 By Legal Obligation

People where there is a legal obligation on the Charity to collect, process and share information with a third party – *eg:* the legal obligations to collect, process and share with HM Revenue & Customs payroll information on employees of the Charity.

The information provided will be held, processed and shared with others solely for the purpose meeting the Charity's legal obligations.

Employees (Human Resources)

Taxation (HM Revenue & Customs)

For the purpose of managing an employee's PAYE and other taxation affairs the information collected will additionally contain details, as required by HM Revenue & Customs, of:

a) The person's National Insurance Number;

b) The person's taxation codes;

c) The person's salary/wages, benefits, taxation deductions & payments;

d) Such other information as may be required by HM Revenue & Customs.

Pensions

For the purpose of managing an employee's statutory pension rights the information collected will additionally contain details, as required by the Charity's pension scheme (National Employees Savings Trust, NEST), of:

a) The person's National Insurance Number;

b) The person's salary/wages, benefits, taxation & payments;

c) Such other information as may be required by the NEST scheme.

4.4 By Vital Interest

The Charity undertakes no activities which require the collection, holding and/or processing of personal information for reasons of vital interest.

4.5 By Public Task

The Charity undertakes no public tasks which require the collection, holding and/or processing of personal information.

4.6 Legitimate Interest

Volunteers, Including Trustees

In order to be able to operate efficiently, effectively and economically, it is in the legitimate interests of the Charity to hold such personal information on its volunteers and trustees as will enable the Charity to communicate with its volunteers on matters relating to the operation of the charity, eg:

- ☑ the holding of meetings;
- ☑ providing information about the Charity's activities – particularly those activities which, by their nature, are likely to be of particular interest to individual volunteers/trustees;
- ☑ seeking help, support and advice from volunteers/trustees, particularly where they have specific knowledge and experience;
- ☑ ensuring that any particular needs of the volunteer/trustee are appropriately and sensitively accommodated when organising meetings and other activities of the Charity.

5. Individual Rights

Note: The following clauses are taken primarily from the guidance provided by the Office of the Information Commissioner,
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

5.1 The right to be informed {Arts 12-14}

When collecting personal information the Charity will provide to the data subject free of charge, a Privacy Policy written in clear and plain language which is concise, transparent, intelligible and easily accessible containing the following information:

- ☑ Identity and contact details of the controller
  Note: where the organisation has a controller's representative and/or a data protection officer, their contact details should also be included
- ☑ Purpose of the processing and the lawful basis for the processing
- ☑ The legitimate interests of the controller or third party, where applicable
- ☑ Categories of personal data
  Not applicable if the data are obtained directly from the data subject
- ☑ Any recipient or categories of recipients of the personal data
- ☑ Details of transfers to third country and safeguards
- ☑ Retention period or criteria used to determine the retention period
- ☑ The existence of each of data subject's rights
- ☑ The right to withdraw consent at any time, where relevant
- ☑ The right to lodge a complaint with a supervisory authority

- ☑ The source the personal data originates from and whether it came from publicly accessible sources
  Not applicable if the data are obtained directly from the data subject
- ☑ Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
  Not applicable if the data are NOT obtained directly from the data subject
- ☑ The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

In the case of data obtained directly from the data subject, the information will be provided at the time the data are obtained.

In the case that the data are not obtained directly from the data subject, the information will be provided within a reasonable period of the Charity having obtained the data (within one month), ***or,*** if the data are used to communicate with the data subject, at the latest, when the first communication takes place***; or***
if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

5.2 The right of access {Art:15}

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed, and, where that is the case, access to his/her personal data and the information detailed in the Charity's relevant Privacy Policy:

5.3 The right to rectification {Art:16}

The data subject shall have the right to require the controller without undue delay to rectify any inaccurate or incomplete personal data concerning him/her.

5.4 The right to erase {The right to be forgotten} {Art:17}

Except where the data are held for purposes of legal obligation or public task (4.3 or 4.5) the data subject shall have the right to require the controller without undue delay to erase any personal data concerning him/her.
Note: This provision is also known as "The right to be forgotten".

5.5 The right to restrict processing {Art:18}

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

5.6 The right to data portability {Art:20}

Where data are held for purposes of consent or contract (4.1 or 4.2) 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.

5.7 The right to object {Art:21}

a) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him/her 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 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.

5.8 Rights in relation to automated decision making and profiling. {Art:22}

Except where it is: a) based on the data subject's explicit consent, *or b)* necessary for entering into, or performance of, a contract between the data subject and a data controller; the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her.

Operational Policies and Procedures

6. Operational Policies & Procedures – The Context

Creative Futures (UK) Limited is a small charity holding just a small amount of non-sensitive data on a small number of people.

The Trustees understand and accept their responsibility under the EU General Data Protection Regulation (GDPR) to hold all personal data securely and use it only for legitimate purposes with the knowledge and approval of the data subjects.

By the following operational policies and procedures the Trustees undertake to uphold the principles and requirements of the GDPR in a manner which is proportionate to the nature of the personal data being held by the Charity. The policies are based on the Trustees' assessment, in good faith, of the potential impacts on both the Charity and its data subjects of the personal data held by the Charity being stolen, abused, corrupted or lost.

7. Personnel

7.1 Data Protection Officer

In the considered opinion of the Trustees the scope and nature of the personal data held by the Charity is not sufficient to warrant the appointment of a Data Protection Officer.

Accordingly, no Data Protection Officer is appointed.

7.2 Data Controller

The Board of Trustees is the Data Controller for the Charity.

7.3 Data Processor

The management team of the Charity, or other appropriate persons as appointed by the management team including third parties such as Mailchimp and higher education institutions, are appointed to be the Data Processors for the Charity.

7.4 Access to Data

Except where necessary to pursue the legitimate purposes of the Charity, only the Data Processors shall have access to the personal data held by the Charity.

7.5 Training

The Board of Trustees and Data Processors will periodically undergo appropriate training commensurate with the scale and nature of the personal data that the Charity holds and processes under the GDPR.

8. Collecting & Processing Personal Data

The Charity collects a variety of personal data commensurate with the variety of purposes for which the data are required in the pursuit of its charitable objects.

All personal data will be collected, held and processed in accordance with the relevant Data Privacy Notice provided to data subjects as part of the process of collecting the data.

A Data Privacy Notice will be provided, or otherwise made accessible, to all persons on whom the Charity collects, holds and processes data covered by the GDPR. The Data Privacy Notice provided to data subjects will detail the nature of the data being collected, the purpose(s) for which the data are being collected and the subjects rights in relation to the Charity's use of the data and other relevant information in compliance with the prevailing GDPR requirements.

9. Information Technology

9.1 Data Protection by Design/Default

Inasmuch as:

a) none of the Charity's volunteer Trustees are data protection professionals;

b) it would be a disproportionate use of charitable funds to employ a data protection professional, given the scale and nature of the personal data held by the Charity;

the Trustees will seek appropriate professional advice commensurate with its data protection requirement whenever:

c) they are planning to make significant changes to the ways in which they process personal data;

d) there is any national publicity about new risks (*eg:* cyber attacks)

which might adversely compromise the Charity's legitimate processing of personal data covered by the GDPR.

Personal data will never be transmitted electronically (*eg:* by e-mail) unless securely encrypted.

9.2 Data Processing Equipment

The scale and nature of the personal data held by the Charity is not sufficient to justify the Charity purchasing dedicated computers for the processing of personal data.

Data will be processed on the computers/laptops to which the Data Processors have access, and stored on the charity's hard drive on Dropbox.

When not in use the computers/laptops will be kept securely and reasonably protected against accidental damage, loss, avoidable theft or other misuse by persons other than the Data Processors.

9.3 Data Processing Location

The Charity's data processors shall only process the Charity's personal data in a secure location, and not in any public place, *eg:* locations whether the data could be overlooked by others, or the computer/laptops would be susceptible to loss or theft.

Computers/laptops in use for data processing will not be left unattended at any time.

9.4 Data Backups

To protect against loss of data, all the Charity's personal data is backed up on its Dropbox server.

9.5 Obsolete or Dysfunctional Equipment
(Disposal of Removable Storage Media)

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.

Equipment which becomes obsolete or dysfunctional shall not be disposed immediately. Instead it will be stored securely while up-to-date methods for its data cleansing and disposal can be sought and implemented.

10. Data Subjects

10.1 The Rights of Data Subjects

In compliance with the GDPR the Charity will give data subjects the following rights.
These rights will be made clear in the relevant Data Privacy Notice provided to data subjects:

- ☑ the right to be informed;
- ☑ the right of access;
- ☑ the right to rectification;
- ☑ the right of erasure *{LO}* *Also referred to as "The right to be forgotten"*
- ☑ the right to restrict processing;
- ☑ the right to data portability; *{LO}* *{LI}*
- ☑ the right to object; *{SC}* *{Co}* *{LO}*
- ☑ the right not to be subjected to automated decision making, including profiling.

The above rights are not available to data subjects when the legal basis on which the Charity is holding & processing their data are: *{SC}* Subject Consent; *{Co}* Contractual obligation *{LO}* Legal Obligation *{LI}* Legitimate Interest

10.2 Rights 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 quickly.

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.

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.

10.3 Right of Portability

The Charity will only provide copies of personal data to the subject (or the subject's legal representative) on written request.

The Charity reserves the right either:

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

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

10.4 Data Retention Policy

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 the Charity holding their data;

b) in the case of data held by legitimate interest of the charity:
the period for which that legitimate interest applies. For example: in the case of data subjects who held a role, such as a freelance practitioner, with the Charity the retention period is that for which the Charity reasonably has a legitimate interest in being able to identify that individual's role in the event of any retrospective query about it;

c) in the case of data held by legal obligation:
the period for which the Charity is legally obliged to retain those data.

The Charity 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.

11. Privacy Impact Assessment

11.1 Employees' and freelancers' Data

The volume of personal data is very low-moderate: around 200 individuals
The sensitivity of the data is moderate: the most sensitive data being bank account details, National Insurance number, address and contact details;
The risk of data breach is medium, as bank details are encrypted on the bank's own system, and held in our password protected server.

Overall impact: MEDIUM

11.2 Volunteers'/Trustees' Data

The volume of personal data is low – less than 10 individuals
The sensitivity of the data is low: the most sensitive data being date of birth, previous names, previous addresses, and contact details;
The risk of data breach is small – primarily the accidental disclosure of names & e-mail addresses.

Overall impact: LOW

11.3 Clients' & Funders' Data

The volume of personal data is low.

The sensitivity of the data is low: the most sensitive data being an e-mail address;
The risk of data breach is small – primarily the accidental disclosure of names & e-mail addresses.

Overall impact: LOW

11.4 Participants' Data

The volume of personal data is moderate.

The sensitivity of the data is moderate: for some projects we collect data (with appropriate permission) regarding participants' age, sex, school, and outcome-related information for reporting and monitoring, and sometimes for research, purposes. This can include some sensitive data.

The risk of data breach is low-moderate: all parties involved in any data processing follow strict guidance, and all data is anonymised in reporting and research analysis.

Overall impact: MODERATE

12. Third Party Access to Data

Under no circumstance will the Charity 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.

Whenever possible, data subjects will be informed in advance of the necessity to share their personal data with a Third Party in pursuit of the Charity's objects.

Before sharing personal data with a Third Party the Charity will take all reasonable steps to verify that the Third Party is, itself, compliant with the provisions of the GDPR and confirmed in a written contract. The contract will specify that:

- ☑ The Charity is the owner of the data;
- ☑ The Third Party will hold and process all data shared with it exclusively as specified by the instructions of the Data Controller;
- ☑ The Third Party will not use the data for its own purposes;
- ☑ The Third Party will adopt prevailing industry standard best practice to ensure that the data are held securely and protected from theft, corruption or loss;
- ☑ The Third Party will be responsible for the consequences of any theft, breach, corruption or loss of the Charity'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
- ☑ 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;
- ☑ The Third Party will securely delete all data that it holds on behalf of the Charity once the purpose of processing the data has been accomplished.
- ☑ The Charity does not, and will not, transfer personal data out of the EU.

13. Data Breach

In the event of any data breach coming to the attention of the Data Controller the Trustees will immediately notify the Information Commission's Office.

14. Privacy Policy & Privacy Notices

The Charity will have a Privacy Policy and appropriate Privacy Notices which it will make available to everyone on whom it holds and processes personal data, in accordance with 5.1.

In the case of data obtained directly from the data subject, the Privacy Notice will be provided at the time the data are obtained.

In the case that the data are not obtained directly from the data subject, the Privacy Notice will be provided within a reasonable period of the Charity having obtained the data (within one month), ***or,*** if the data are used to communicate with the data subject, at the latest, when the first communication takes place***; or***
if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.