Creative Royston
Data Protection Policy Statement

Definitions

Organisation	means Creative Royston a not-for-profit organisation
GDPR	means the General Data Protection Regulation.
CRMC	means the Creative Royston Management Committee
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Organisation.
Responsible Person	means the Website Administrator who is the person voluntarily dealing with Data Protection issues on behalf of the Organisation

1. Data protection principles

The Organisation takes their role as a Data Controller seriously and to that end is committed to processing data in accordance with its responsibilities under the GDPR and, in particular, to abiding by the six principles relating to the processing of personal data described in Article 5 below.

Article 5 of the GDPR requires that personal data shall 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."

2. General provisions

a. This policy applies to all personal data processed by the Organisation.

Document reviewed: May 2018
Next review date: May 2019 or when legislation changes, if earlier.

b. The Responsible Person shall endeavour to ensure the Organisation's ongoing compliance with this policy and data protection issues based on active support and endorsement from the other members of the CRMC.

c. This policy shall be reviewed at least annually.

d. the Organisation is not-for-profit and processes personal data in a manner that qualifies for an exemption from the requirement to register with the Information Commissioner's Office (ICO) for Data Protection purposes. The terms of the exemption are explained in Section 6 of the ICO Registration self-assessment tool which can be found on the ICO website. The Organisation has chosen to register voluntarily and still has an obligation to adhere to the principles of the Data Protection Act (1998), the GDPR and successive legislation, and will take all reasonable and proportionate steps to ensure that your personal data is kept secure against unauthorised access, loss, disclosure or destruction.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent an organisation may choose to maintain a Register of Systems. Owing to the nature of systems used by the Organisation, a description of them and the contexts in which personal data is processed is fully explained within the Organisation's Privacy Notice.

b. The Organisation's Privacy Notice shall be reviewed at least annually.

c. Individuals have the right to access their personal data and any such requests made to the Organisation shall be dealt with in a timely manner as described in the Privacy Notice.

4. Lawful purposes

a. All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.

b. the Organisation shall note the appropriate lawful basis in its Privacy Notice.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems.

5. Data minimisation

The Organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. the Organisation shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b. The archiving policy shall consider what data should/must be retained, for how long, and why.

Document reviewed: May 2018
Next review date: May 2019 or when legislation changes, if earlier.

c. The archiving policy is explained within the Organisation's Privacy Notice.

8. Security

a. The Organisation does not possess any IT equipment of any description and does not supply or otherwise provide (directly, or indirectly e.g. by reimbursement of cost) IT equipment to CRMC members with the exception of occasionally reimbursing members purchasing USB sticks for the purpose of storing the data processed by the Organisation as explained later in this document. It follows that the Organisation employs mainly operational measures to ensure that personal data is stored securely rather than by using modern software that is kept-up-to-date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Backup and disaster recovery solutions shall be in place as appropriate but taking account of the need to avoid the further unnecessary dissemination of personal data.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people’s rights and freedoms and if appropriate report this breach to the ICO.

END OF DOCUMENT

Document reviewed: May 2018
Next review date: May 2019 or when legislation changes, if earlier.