Personal Data Protection
Policy 7.02

Adoption-Approved by the Executive Committee of CCA Trustees

Signed/ Date……Richard Smith /May 3rd…….. Chairman

Revision – Reason and Date– to be determined by responsible party

Code(B-Z)	Reason for Amendment	Approved By:	Date

Purpose – Ensures CCA meets the requirements of U.K. data protection law.

Additional Authority – General Data Protection Regulations (GDPR) May 2018.

Scope – All personal data as defined in the GDPR held by CCA

Responsible Party –Trustee nominated as Lead Trustee

Policy Statement – Ensures that the CCA meets its legal obligations to protect all personal data it holds, such data being judged necessary to conduct the CCA business.

Procedures-
General public
1. Review what types of personal data are being held, or may be held in future.

2. Define which data needs to be protected. Examples may include:

- Information on applicants for posts, including references.
- Members – contact details, such as name, addresses, phone, e-mail addresses
- In many CCA sections and affiliated organizations, contact details, bank account number
- Users – contact details, such as name, addresses, phone, e-mail addresses, bank account number

3. Appoint member of staff to act as GDPR Data Controller/Processor, normally the CCA Centre manager
4. Arrange for secure data storage, either in hard copy or electronic form. Hard copy to be stored in locked filing cabinets, and electronic storage on the CCA office computer equipment, with up-to-date security software, and password protected.
5. Communicate to the individuals concerned as to the need for the CCA to hold such data, and seek and record their permission to hold the data in a protected manner
6. Collect data from individuals such as name, addresses, phone, e-mail addresses and store securely.
7. If so requested release the data to the individual.
8. If the data is no longer required, ensure it is comprehensively destroyed

Employees

1. Review what types of personal data are being held, or may be held in future. Examples may include
- contact details, such as name, addresses, phone, e-mail addresses
- bank account number,
- payroll information,
- supervision and appraisal notes,
- contracts of employment,
- records of remunerations,

2. Arrange separate secure storage from general public personal data. Hard copy to be stored in locked filing cabinets, and electronic storage on the CCA office computer equipment, with up-to-date security software, and password protected.

3. Collect data about individuals and store securely

4. Communicate to the individuals concerned as to the need for the CCA to hold such data, and seek and record their permission to hold the data in a protected manner

5. If so requested release the data to the individual

6. If the data is no longer required, ensure it is comprehensively destroyed