

# CCPE

## GDPR Policy, including Key Procedures

### Aims of this Policy

CCPE needs to keep certain information on its:

- employees, contracted personnel, volunteers
- trainers
- students
- customers
- clients
- professional experts and advisers and consultants
- members of exam boards
- supporters
- suppliers
- authors, publishers and other creators
- third parties participating in course work
- complainants, enquirers
- representatives of other organisations
- individuals captured by CCTV images
- persons who may be the subject of an enquiry
- auditors
- members of the public and people in the area which is under CCTV surveillance
- legal representatives
- local and central government

to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

We process personal information to enable us to:

- provide a voluntary service for the benefit of the national public as specified in our constitution
- provide help and advice on voluntary services
- provide education, training, welfare and educational support services
- administer college property
- administer library services
- administer membership records
- provide mental health counselling and psychotherapy
- provide commercial activities to our clients
- offer a mediation service
- advertise and promote the Charity/College and the services we offer
- undertake research
- fundraise and promote the interests of the charity
- support and manage our employees and volunteers
- maintain our own accounts and records
- Our processing also includes the use of CCTV systems to monitor and collect visual images for the purposes of security and the prevention and detection of crime

CCPE is committed to ensuring any personal data will be dealt with in line with the General Data Protection Regulation (GDPR) 2016. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the CCPE organisation.

This policy covers students, employees, self-employed and freelance staff, members, clients & service users, volunteers, trustees and suppliers.

## Definitions

In line with the GDPR principles, CCPE will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.:

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the GDPR's data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

## **Type of information processed**

CCPE processes the following personal information and may include:

- personal details
- family details
- lifestyle and social circumstances
- membership details
- goods and services
- financial details
- education details and student records
- education and employment details
- disciplinary and attendance records
- vetting checks
- visual images, personal appearance and behaviour (CCTV)

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- sexual life
- religious or other beliefs of a similar nature
- offences and alleged offences
- criminal proceedings, outcomes and sentences

Personal information is kept in the following forms:

- Paper based and computer-based systems.

Groups of people within the organisation who will process personal information are: students, employees, self-employed and freelance staff, volunteers and trustees.

## **Notification**

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires.

If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is Alice Williams.

## **Responsibilities**

Under the GDPR, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of CCPE this is the Board of Trustees

The governing body delegates tasks to the Data Controller. The Data Controller is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes

All employed staff, self-employed and freelance staff, students, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

The Board of Trustees are accountable for compliance of this policy.

Any unauthorised disclosure or breach of this policy by members of staff will result in disciplinary proceedings. Any unauthorised disclosure made by a student may result in the termination of training. Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement. Any unauthorised disclosure by a supplier will break the terms of contract and legal proceedings will be instigated.

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

### **Policy Implementation**

To meet our responsibilities staff, self-employed and freelance staff, students, trustees and volunteers will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

### **Training**

Training and awareness raising about the GDPR and how it is followed in this organisation will take the following forms:

On induction staff are provided with:

- this GDPR policy document which they are asked to sign.
- guidelines on how to store data in both hard and electronic copy.

General training/ awareness raising:

- All paperwork regarding the GDPR is provided for staff and students on our online portals.
- Annual reminders are sent out to all staff, self-employed and freelance staff, students, trustees and volunteers.
- Any and all staff meetings will carry reminders of the importance of compliance with GDPR.

## **Gathering and checking information**

Before personal information is collected, we will consider the GDPR principles and ensure we adhere to them. We will only gather information that is relevant to the needs of the data subject and the organisation.

We will inform people whose information is gathered about why we require their data and how we will use it. In the case of students, for example, we gather their data in order to track their experience with us and to ensure we maintain contact with them throughout the duration of the course they attend. They will be informed about who will have access to their information over the course of their time with us. All data gathered will be accompanied with an explanation.

We will take the following measures to ensure that personal information kept is accurate:

- regular reminders will be issued to students via the student portal and via the teaching staff
- for those who work for CCPE in any capacity, they themselves and their line managers will be responsible for ensuring information is up to date.

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

## **Data Security**

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Using lockable cupboards with restricted access to keys.
- Computer systems allow restricted access to database systems.
- Not allowing personal data to be taken off site as hard copy, on laptop or on memory stick unless the portable device is password protected and encrypted.
- Back-up of data on computers.
- Encrypted and password protected attachments for sensitive personal information sent by email.
- Paper-based information is destroyed by an onsite shredder or by a confidential waste supplier.

Any unauthorised disclosure or breach of this policy by members of staff will result in disciplinary proceedings.

Any unauthorised disclosure made by a student may result in the termination of training.

Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

Any unauthorised disclosure by a supplier will break the terms of contract and legal proceedings will be instigated.

## **Subject Access Requests**

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the GDPR

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to:

*The Data Controller  
Operations Manager  
CCPE  
Beauchamp Lodge  
2 Warwick Crescent  
London W2 6NE*

The following information will be required before access is granted:

- Full name and address
- Relationship with CCPE

We may also require proof of identity before access is granted. The following forms of ID will be required:

- Passport
- Recent proof of address eg Utility bill

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within the 30 days required by the GDPR from receiving the written request and relevant fee.

### **Review**

This policy will be reviewed at intervals of no more than 2 years to ensure it remains up to date and compliant with the law.

### **Declaration**

I confirm I have read and understood CCPE's General Data Protection Regulation Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a: *[tick as appropriate]*

- Member of staff *[PAYE, self-employed or freelance]*
- Student
- Volunteer
- Trustee/ management committee member
- Other, specify:

Signature: \_\_\_\_\_

Print name: \_\_\_\_\_

Date: \_\_\_\_\_

Please return this form to: **Alice Williams, Operations Manager, [data@ccpe.org.uk](mailto:data@ccpe.org.uk)**