The only awarding body run *by* counsellors

2024 - 2025

CPCAB Data Protection Policy

CPCAB Data Protection Policy

1. Introduction

CPCAB is licensed in accordance with the legal requirements of the UK General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. This means we follow strict procedures specified by this legislation when collecting and handling personal data about individuals. We are registered with the Information Commissioner's Office (ICO) as CPCAB Ltd (this is our 'Data Controller Name'). Our registration number (also known as our notification number) is Z6708416.

2. Privacy Notice

All personal information data held by CPCAB must be:

- fairly and lawfully processed, for relevant purposes only;
- secure, accurate and up to date;
- not kept longer than necessary;
- processed in accordance with an individual's rights.

We will only share your personal data with other organisations where there is a clear requirement to do so. We will never pass on your details to other companies for marketing purposes. These organisations, who are themselves subject to data protection legislation, may include:

- The Learning Records Service (LRS);
- Ofqual, Qualifications Wales or CCEA Regulation;
- Education and Skills Funding Agency (ESFA);
- A court of law under direction;
- The British Association for Counselling and Psychotherapy (BACP);
- An external supplier for the sole purpose of fulfilling a contract such as printing certification for qualification completion.

3. Fair Processing of Data

We process data on behalf of candidates, centre staff and CPCAB staff. The purposes for gathering this data are known under GDPR law as "lawful bases" and include:

- Performance of a contract with the data subject;
- Compliance with legal obligations;
- Occasionally other lawful bases may also be relevant.

An internal Data Retention Policy lists individual pieces of data with the rationale for processing them, a retention period, a description of its format and how consent was obtained.

3.1 CPCAB and UK GDPR/DPA 2018

The section below provides more information on how we work to the highest standards in protecting the data of our centres and candidates.

As an awarding organisation we retain and make available to our regulators assessment materials for each qualification in the following ways:

- Registration records of all candidates from all centres.
- Records of verification, including sampling records and reports from all centres.
- Centres may be requested to supply examples of candidate work to the awarding organisation (or regulator) for purposes of ongoing monitoring of standards. These may be copied and retained, but originals will be returned. This material will remain confidential to the awarding organisation and regulators unless specific permission is obtained from the centre/candidate for it to be used for training and/or standardisation purposes.
- Records of all results, and details of all certificates issued to registered candidates.
- Records of all reasonable adjustments, special considerations, enquiries, complaints and appeals.
- All data specified and requested by the regulators will be supplied.

4. Security of Data

4.1 Rectification of your Data (see also section 5, Subject Access Requests)

Candidate data is gathered by the centre and requests to make alterations may be accepted up to the point of certification[1]. Please note that after this time certificates can only be re-printed in a different name where the candidate is initiating a new identity, for example as part of gender reassignment. This policy is designed to ensure the integrity of the qualification and to prevent fraud.

Tutor data is gathered by the centre and relevant data is forwarded to CPCAB via the online tutor CV template. Tutors are requested to check periodically that the data held by CPCAB remains accurate.

Staff data, including for external consultants and actors (who are required to sign a separate release form relating to their filmed material), may be amended at any point on request; supporting information may be required as appropriate.

Marketing information (email addresses) may be amended on request at any time.

4.2 Deletion of your Data

You can request that the data we hold on your behalf is deleted. In the absence of such a request, candidate data is retained over time to monitor standards, prevent fraud and provide replacement certificates. To facilitate compliance with our responsibilities and uphold standards set by government authorities, we will retain a minimum of data to check the validity of certificates and track qualification completion.

Candidates are reminded that if you request to have your data deleted it may not be possible to issue a replacement certificate in the future or to verify your achievement. A request to delete data may be refused if it is required to provide data to regulatory authorities or as part of a direction from a court of law.

4.3 Data Breaches

[1] *Where a centre has failed to request rectification of a candidate's name before this point a replacement certificate can only be issued in the new name where there is clear evidence to support the case, such as a formal confirmation that the centre was provided with change of name via an enrolled deed poll during the course. Our replacement certificate fee will apply in such cases. See our fees webpage for further details.*

We take our data retention responsibilities seriously and we will handle any data breach promptly, thoroughly and transparently. In the event of a data breach we will:

- Identify the scale of the breach no later than 48 hours after becoming aware of it and
- Identify the sensitivity of the data as well as its potential impact on the data subject.

Depending on the outcome, we will, if appropriate:

- Notify the ICO
- Notify the Police
- Notify our regulators
- Notify the data subject(s)
- Formally record any lessons learned
- Initiate an appropriate action plan, such as extra security measures or staff training.

4.4 Data Portability

Under the UK GDPR and the Data Protection Act 2018 you can apply for your own data to be provided to you in a format that will allow you to share it with another organisation, such as a different awarding organisation. In practice the data we hold on you is limited and we recognise that it's unlikely that this service will be helpful to you but do please get in touch if you'd like to explore this option.

4.5 General Security

We operate a range of processes to ensure that the data we process is retained securely. They include, amongst others:

- Staff computers are password protected and run on the latest software patches with up-to-date antivirus protection.
- Sensitive documents are further password protected, for example staff annual reviews, financial documents etc.
- We have implemented a mandatory multi-factor authentication policy. All staff members are required to have multiple security levels for data access.
- We continue to adhere to all requirements for the Cyber Essentials security certification.
- SAR requests and replacement certificates require a range of ID to be submitted in support of each request.
- Payments for online sales, e.g. support videos are processed by UK GDPR and DPA 2018-compliant service providers.

There is a separate internal policy that relates to the procedures that apply when a member of staff leaves our employment.

4.6 Data Storage Equipment

Redundant equipment does not leave our premises until all the files stored – whether they contain personal data or not – have been permanently erased beyond any possibility of retrieval. In the case of hard disks, for example, this means securely re-formatting each disk. Redundant data storage devices are rendered physically useless before disposal. Any redundant hard copy which contains personal data is also destroyed securely.

5. Subject Access Requests

We acknowledge your right to be informed by us whether your personal data is being processed by us and, if so, to be given by us a description of the personal data involved and the purposes for which it is being (or is to be) processed.

You can apply for copies of your personal data under the Subject Access Request (SAR) scheme. SAR requests must be received in writing and copies of the data will be provided electronically. If you are unable to access an electronic response please let us know and we will take appropriate steps to facilitate a response.

Under the Data Protection Act (2018) organisations are not required to disclose marked scripts (external assessment papers) to applicants. In other words, candidates have no right of access to marked scripts (EA papers). Information recorded by candidates during an academic, professional or other examination is exempt from the scheme and it is our policy not to disclose candidate scripts (exam papers) to candidates. Other material including assessors' comments can be requested, although please be aware that we operate an internal archiving policy and assessment materials are securely destroyed after a defined period of time.

We will remove any references that might allow another individual to be identified, unless that person has consented (in writing) to such a disclosure. If it is not possible to provide copies of any other information, for example because to do so would identify another person and compromise their rights to confidentiality, you will be given an explanation of the decision.

We will respond to such requests within one month. Please be aware that we reserve the right to refuse any requests that may be considered excessive or manifestly unfounded. The data you provide as part of a SAR request will be retained securely as proof that we have followed due process when responding to the request. We request ID to satisfy our requirement to confirm the identity of the requester (or the person the request is made on behalf of). Please note that the timescale for responding to a SAR does not begin until CPCAB has received the requested information set out on the online form.

To submit a SAR please use our online form to help us process your request as efficiently as possible.

6. CPCAB's Recognised Centres

Centres approved to offer CPCAB qualifications are responsible for gathering data on candidates and tutors, some of which is shared with us. For the purposes of the data privacy laws, CPCAB and its centres are independent data controllers and have an equal obligation to be compliant with General Data Protection Regulations.

Centres are also reminded to take special care where any recordings are made of counselling skills or practices, because they may contain sensitive material revealed by the candidate, although candidates should bear in mind that their work is designed to be used as assessment material and may be viewed by others, such as our External Verifiers.

In a legal challenge, although rare, it may be necessary to share sensitive data with a court of law, which has the power to overrule GDPR.

Our Archiving and Retention Policy for Centres explains the retention periods for centres and the rationale behind the decisions.

7. CPCAB's websites

In general, you can browse CPCAB's websites without disclosing any information about yourself. If you visit CPCAB's websites to read or download information, we collect and store only the following information that is automatically recognised: the date and time, the originating IP address, the domain name, the type of browser and operating system used (if provided by the browser), the URL of the referring page (if provided by the browser), the object requested and the completion status of the request.

7.1 Cookies and Other Technologies

As described above, we sometimes collect anonymous information from visits to our site to help us provide better customer service. For example, we keep track of the domains from which people visit and we also measure visitor activity on CPCAB's websites, but we do so in ways that keep information anonymous. We use the information that we collect to measure the number of visitors to the different areas of our site, and to help us make the site more useful to visitors. This includes analysing these logs periodically to measure the traffic through our servers, the number of pages visited and the level of demand for pages and topics of interest. The logs may be preserved indefinitely and used at any time and in any way to prevent security breaches and to ensure the integrity of the data on our servers.

We collect the anonymous information we mentioned above through the use of various technologies, one of which is called "cookies". A cookie is an element of data that a website can send to your browser, which may then be stored on your hard drive. For example, on a website with a login system (if users register for it), cookies are used to save the visitor's password so that it does not have to be entered at each new visit.

This anonymous information is used and analysed only at an aggregate level to help us understand trends and patterns. None of this information is reviewed at an individual level. If you do not want any transaction details used in this manner, you can disable your cookies.

7.2 Links

Throughout CPCAB's websites, you will find links to third party websites. Please note that CPCAB is not responsible for the privacy policies or content on third party websites.

8. Your Right to Complain

You can complain about the data held by us on your behalf if it is:

- Inaccurate. Please note that it is the responsibility of centre staff to upload personal data to the CPCAB Portal on behalf of their candidates and inaccurate information may lead to incorrectly printed certificates and/or failure to upload Learner Achievement Data. See also footnote, page 1.
- Inappropriate. If you feel that it is not appropriate for us to hold any of your personal information, please liaise with us (if you are a tutor) for advice. If you are a candidate, please liaise with your tutor.

- Insecure. Data held by us is securely stored (see section 4, above) but candidates should be aware that their work both within their centre and in external assessment is regarded as assessable material and may be seen by others.

For further information from us please contact contact@cpcab.co.uk (please mark "for the attention of the Data Protection team").

For further information (or queries) about the Act:

- Office of the Data Protection Commissioner
  Wycliff House, Water Lane
  Wilmslow, Cheshire SK9 5AF
- Tel: 0303 123 1113
- Email: mail@dataprotection.gov.uk
- Web: https://ico.org.uk/

For the data protection and privacy policies of CPCAB's regulators:

- Ofqual
- Qualifications Wales
- CCEA

For the data protection of CPCAB's partners:

- ESFA
- Open University
- Learning Records Service

CPCAB 2024