Data Protection Policy and Procedure & GDPR

Please note that these procedures are also in conjunction with P&P041, P&P042, P&P043

Contents

Introduction

Purpose and Scope

Construction & Plant Assessments (CPA) is committed to the protection of individuals' rights and privacy in accordance with the Data Protection Act 2018 ("the Act") and General Data Protection regulation. This Policy has been developed to provide detailed guidance on the correct and lawful processing of personal data, to ensure that all staff, learners, and other workers who process personal data on behalf of CPA are doing so in accordance with the Data Protection principles. The Policy applies to all staff, learners, suppliers, and others with whom CPA has dealings. A breach of the Data Protection Policy by members of staff or learners will be considered as a disciplinary offence and will be dealt with in accordance with CPA's disciplinary procedures. In addition, a breach of the Policy may expose CPA and individual concerned to criminal or civil liabilities. In addition to any CPA liability, staff may also be personally liable. Data subjects may also apply to court for compensation if they have suffered damage from such a loss.

General Policy Statement

Construction and Plant Assessments need to process certain personal information about its staff and learners in order to fulfil its purpose and to meet its legal obligations to funding bodies and the government. The processing of personal information such as collection, recording, use, and storage of personal information must be dealt with lawfully and correctly in accordance with the Data Protection Act 2018. All information containing personal data must be protected against unauthorised access, accidental loss or destruction, modification or disclosure. CPA regards the lawful and correct treatment of personal information as important to its successful operation, and to maintain confidence between those with whom we deal and ourselves.

SQA Secure Site

The Head of Centre holds sole responsibility for ensuring processes are in place to maintain the security of the materials published on the SQA Secure Site.
Any suspected breach of the site will be reported to SQA immediately.
In the event of a breach or any other member of Construction & Plant Assessment gaining access to the username and password for the site, the Head of Centre must request a new username from SQA and create a new password.

Definitions

Personal Data

"Personal Data" means data relating to a living individual who can be identified: -

- from that data; or
- from that data and other information, which is in the possession of, or is likely to come into the possession of, the data controller.

Personal data can be either factual (such as name, address, telephone, images, and photographs) or an expression of opinion about the individual (such as a performance appraisal or comments on scripts) including any intentions of the data controller or any other person in respect of that individual. Personal data covers any information which relates to an individual in any format (written or oral). Examples include:

- a learner or staff file
- an email about someone
- a post-it note with someone's name and telephone number.
- Information provided orally about the learner's personal circumstances.

Sensitive Data

"Sensitive Personal Data" consists of personal data relating to:

- ethnic origin,
- physical and mental health (including, for example, details of the reasons for an individual's sick leave),

- sex life,
- religion or belief,
- political opinion
- information relating to alleged or actual criminal offences.
- Trade Union membership

The more 'sensitive' the nature of the data the more securely it should be treated in terms of deciding whether it is necessary to obtain it, the method of obtaining it, whether to retain/disclose it and how to retain/disclose it.

Processing
"Processing" means obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data.

Data Subject
"Data subject" means an individual who is the subject of the personal data.

Data Controller
"Data controller" means a person who or organisations which (either alone or jointly or in common with other persons/organisations) determines the purposes for which, and the manner in which, any personal data is processed. In this case, this means CPA or nominated individuals acting on behalf of and with the authority of CPA.

Data Processor
"Data Processor" means any person (other than a member of staff) who processes data on behalf of Construction and Plant Assessments.

Staff
Unless otherwise applicable, all references to staff include all current, past, and prospective staff, full-time, part-time staff, and contractors.

Learners
Unless otherwise applicable, all references to learners include all current, past, and prospective learners, whether full-time or part-time.

What is the Data Protection Act?
The Data Protection Act is concerned with making sure that organisations handle personal data in a responsible way. It sets out legal obligations on how personal data is to be handled in relation to its collection, uses, storage, destruction, transfer, and disclosure.

The Act applies to any information about a living individual (e.g., learners, staff, members, etc). Essentially, staff handle any information about people as part of their job will need to comply with the Data Protection Act.

Data Protection Principles
The 8 principles set out in the Act require that personal data:

I. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
II. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
III. Shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
IV. Shall be accurate and, where necessary, kept up to date.
V. Shall not be kept for longer than is necessary for that purpose or those purposes.
VI. Shall be processed in accordance with the rights of data subjects under the Act.
VII. Shall be protected by appropriate technical and organisational measures which shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
VIII. Shall not be transferred to any country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Conditions for Processing
Before Construction and Plant Assessments can process data it must meet one or more of the conditions for processing which are set out in schedules 2 and 3 to the Data Protection Act.

Unless a relevant exemption applies, at least one of the following conditions in schedule 2 must be met before staff process any personal data:

<u>Schedule 2</u>

<u>Condition 1</u>
The data subject has given their consent to the processing.

<u>Condition 2</u>
Processing is necessary for the performance of a contract or for taking steps for entering into a contract with the data subject.

<u>Condition 3</u>
The processing is required under a legal obligation to which the data controller is subject, other than an obligation imposed by contract.

Condition 4
The processing is necessary to protect the vital interests (matters of life and death) of the data subject.

Condition 5
The processing is necessary:

- for the administration of justice
- for the exercise of any functions conferred on any person by or under any enactment
- for the exercise of any functions of the Crown, a Minister of the Crown, or a Data Protection
- for the exercise of any other functions of a public nature exercised in the public interest by any person

Condition 6
The processing is necessary in order to pursue the legitimate interests of the data controller or third parties, or parties to whom the data are disclosed unless it could prejudice the rights and freedoms or legitimate interests of the data subject.

Sensitive Personal Data
When processing sensitive personal data, one of the following conditions in schedule 3 must also be met in addition to one of the conditions from schedule 2 above:

Schedule 3

Condition 1
The data subject has given his/her explicit consent.

Condition 2
The processing is required by law in connection with employment.

Condition 3
The processing is necessary to protect the vital interests of the data subject or another person.

Condition 4
The processing:

- Is carried out in the course of its legitimate activities by anybody or association which exists for political, philosophical, religious or trade union purposes and which is not established or conducted for profit.
- Is carried out with appropriate safeguards for the rights and freedoms of data subjects.
- relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes; and
- does not involve disclosure of personal data to a third party without the consent of the data subject.

Condition 5
The information has been made public by the data subject.

Condition 6
The processing is necessary for legal proceedings, obtaining legal advice, or establishing or defending legal rights.

Condition 7
The processing is required for the administration of justice, the exercise of functions under an enactment, or the exercise of functions of the Crown or a government department.

Condition 8
The processing is necessary for medical purposes and is carried out by a health professional or a person with an equivalent duty of confidentiality.

Condition 9
The processing:

- is of sensitive personal data consisting of information as to racial or ethnic origin,
- is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
- is carried out with appropriate safeguards for the rights and freedoms of data subjects.

Condition 10
The personal data is processed in circumstances specified in an order made by the Secretary of State.

Responsibilities Under the Data Protection Act

Construction and Plant Assessments
Construction and Plant Assessments is the data controller and is committed to the protection of rights and privacy of individuals (includes learners, staff, and others) in the processing of personal data.

CPA's Director or other member of the senior team is the appointed Data Protection Officer responsible for the management of data protection matters and for the development of specific guidance on data protection issues for CPA.

The Administration, Quality Controller and Curriculum Manager are responsible for developing and maintaining good information handling practice within CPA in accordance with this Policy. They are also responsible for ensuring that all staff are aware of their responsibilities within Data Protection.

Staff as Processors

All staff or others who process or use any personal data must ensure that they follow the data protection principles and the guidance provided in the Data Protection Policy at all times.

All staff must report any incident, or potential incident, likely to result in unauthorised disclosure, damage, destruction, or loss of Personal Data directly to the Director.

Staff/Learners as Data Subjects

All staff and learners are responsible for:

- Checking that any information that they provide to CPA is both accurate and up to date.
- Informing CPA of any changes to information which they have provided, e.g., changes in addresses; and
- Informing CPA of any errors in the information it holds about them.

Data Protection Training

It is mandatory for key staff to undertake Data Protection Training. On-line E Learning Data Protection training and data protection seminars will be held to assist members of staff with an understanding of their legal duty under the Act. Staff in key roles will be provided with additional Data Protection training.

Data Protection training will be a part of a new member of staff's induction.

Failure to complete any mandatory Data Protection training may give rise to disciplinary action.

Collection and Processing of Personal Data

Whenever personal data is collected, members of staff should make clear to the data subject what purpose(s) the information is be used for and, where necessary, obtain consent to the processing of the data. In most instances consent to process personal data is obtained routinely by CPA (e.g., when a learner signs a registration form or when a new member of staff signs a contract of employment). For sensitive data, explicit written consent must always be obtained from the data subject.

Any CPA forms (whether paper-based or web-based) that gather data on an individual should contain a fair processing notice which explains the following:

- Why the data is being gathered and how the data will be used.
- To whom the data may be disclosed to within CPA and to any outside third parties; - The fact that completion of the form will be taken as consent given to the use of the data as outlined.

Where consent is not provided for certain types of processing (e.g., direct marketing), appropriate action must be taken to ensure that the processing does not take place.

Data collection forms must be approved by the quality controller before they can be used.

Adequate, Relevant and not Excessive

The Act only permits the collection of adequate, relevant, and not excessive amount of personal data. This means that only the personal data required for the specific purpose(s) notified to the data subject should be collected. Any data which is not necessary for that purpose(s) should not be collected.

Processing for Limited Purposes

Staff may only process data for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act and notified to the office. This means that personal data must not be collected for one purpose and then used for another purpose. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

All staff must take care to use personal data held by CPA only for the purposes for which they were primarily intended, e.g.

- Staff, agent, and contractor administration.
- Advertising, marketing, public relations, and general advice service.
- Accounts and records.
- Education.
- Learner and staff support services.
- Research.
- Crime prevention and prosecution of offenders.
- Provision of commercial services.

Data Storage, Retention and Disposal

It is the responsibility of the relevant staff member to ensure that centralised records are maintained to meet the needs and reasonable expectations of the learner, CPA, and external bodies. For members of staff, the Director has the responsibility of ensuring that centralised records are maintained.

Where possible central databases should be used to avoid duplication of information and to increase data security. All local databases maintained by staff in the course of their duties containing personal data (including those using reference numbers for individuals rather than names) must be adequately secure.

CPA is required to ensure that all data is accurate and up to date. Staff and learners have a responsibility to regularly update their records by informing the Quality Controller.

CPA should not retain personal data for longer than is necessary. This means that personal data should be destroyed or deleted when it is no longer required.

Staff should regularly review their records to ensure that the documents they hold are destroyed within the relevant destruction time limit. Where the documentation contains personal information, the destruction must take place confidentially (e.g., shredding, disposal as confidential waste, secure electronic deletion).

Data Security
Each individual must ensure that personal data is processed in accordance with a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. This may mean avoiding use of email in favour of confidential post, the use of passwords or encryption for electronic documents and keeping papers under lock and key.

The need for security is greater where sensitive personal data is involved.

Particular care should be taken when staff are taking personal data off-site from their usual place of work as there is a greater risk of loss, theft, or damage to personal data off-site. The transport of personal data in any format (laptop, hard copy, memory stick etc.) should therefore be avoided as far as possible. This applies especially to sensitive personal data, large volumes of personal data, or information which could cause particular harm or distress if lost. Only in exceptional circumstances should sensitive information be transported outside of CPA's premises. Staff who do so should always ensure that it is kept with them at all times. Staff should:

- Where possible use CPA's PCs to access information as an alternative to transporting data.
- Only carry the minimum amount of personal data (e.g., avoid carrying the whole file if only one document is needed).
- It is CPA's intention that all mobile devices (laptops, smartphones, tablets) and external storage media (USB sticks, external hard drives, DVDs, CDs, etc.) used to transport personal data and sensitive personal data outside CPA will be secured by deploying strong encryption. Their loss/theft must be immediately reported to the Quality Controller.

<u>When working from home staff should:</u>

- Never save documents containing personal data to a personal PC.

<u>Staff Duties</u>
All staff are responsible for ensuring personal data is kept securely and accessible only to those who need to use it. Appropriate security measures are to be taken to prevent accidental loss of, or damage to, personal data.

Staff and others are to ensure that they comply with the security procedure set out below.

Security Procedure:

Electronic Records

1. Care should be taken to ensure that PCs and terminals are not visible to unauthorised persons and that computer passwords are kept confidential.

2. CPA 's Wi-Fi password is kept confidential to staff members only under no circumstances should this password be given to any learner at any time. If a CPA member of staff leaves, the Wi-Fi password is to be changed.

3. PC screens should not be left unattended without password protected screensavers.

4. Personal data should be password protected.

5. Personal data should be encrypted when sent via email.

6. Only encrypted memory sticks should be used to transfer personal data.

Manual Records

7. Manual records should not be left where they can be accessed by unauthorised personnel.

8. Personal data should be kept in a lockable room with controlled access, or in a locked drawer or filing cabinet.

9. Manual records should be shredded or disposed of in "confidential waste" bin provided by CPA for this purpose.

Disclosure

Staff must not disclose personal data to a third party except in limited cases where there is a legal or statutory duty to do so. All staff must therefore take care to ensure that personal data is not disclosed to unauthorised third parties which includes family members of the data subject, friends, government bodies and the Police in certain circumstances without the data subject's consent.

Confirmation of Learner Status

Learner status is regarded as personal data under the Data Protection Act. confirmation of whether or not an individual is a learner of CPA is therefore considered to be unauthorised disclosure of personal data. Disclosing Data to a Third Party

Personal data may only be transferred to third-party processors if they agree to comply with those procedures and policies or have in place adequate measures to do so.

Disclosing Personal Data Overseas

In accordance with Principle 8 of the Data Protection Act, you may not transfer personal data to countries outside of the European Economic Area (EEA) (the European Union Member States along with Iceland, Liechtenstein, and Norway) unless the country or territory has an adequate level of protection for personal data.

Exemptions

There are also exemptions to Principle 8 of the Data Protection Act which enables the transfer of personal data outside of the EEA even if there is no adequate protection. The most likely exemptions applicable to CPA are where:

- The data subject has given explicit consent.
- The transfer is required for the performance of a contract.
- The transfer is necessary for legal proceedings.

However, it is good practice to ensure that there is adequate protection before transferring personal data outside of EEA and only rely on the exemptions if there is no adequate protection.

Rights of Access

Making a Subject Access Request

Staff, learners, and other data subjects about whom CPA holds or uses personal data have a legal right to access that information and request a copy of the data in permanent form by completing a subject request form.

By law, CPA has 40 calendar days from receipt of the request and proof of identity, in which to respond to subject access requests, in any event CPA will endeavour to respond as quickly as possible. In limited circumstances, CPA may not be able to release personal data because exemptions under the Act are applicable, or the disclosure of the data would release personal data relating to other individuals.

CPA is committed to openness and has simpler procedures that allow data subjects access to key data. Current members of staff may view their personnel file, by either making an appointment with the Director or requesting copies of their personnel file.

Learners who wish to access copies of their student files or any other personal data should make a subject access request.

Receiving a Subject Access Request

If you receive a request for personal information from an individual (data subject) or a third party acting on behalf of a data subject, direct them to complete the Subject Access Request form to be submitted to the Director. Where a third party is acting on behalf of a data subject, written authorisation from the data subject must be provided to confirm that the third party is acting on their behalf.

Do not provide any personal information to the data subject or third party, even if you hold such information, unless the request is for information which would normally be released as a matter of routine (e.g., requests for transcripts). All requests for personal information must be processed centrally.

Email Usage

The majority of e-mail communications that staff send or receive will be simple transactions regarding CPA business. Staff should avoid using e-mail to send personal information of a sensitive nature or to express views about individuals. This is because e-mail is an insecure medium and the sender has no control over the storage or use of the message after it has been sent.

Staff who receive by e-mail, from learners or others, information that might be personal data or sensitive personal data should not retain such messages. They should print it out and delete the e-mail from their computer. (examples might include any mention of individuals in relation to discipline or performance, safeguarding, family or personal circumstances.) The printed information should then be kept in the appropriate hard copy filing system in accordance with this Policy and be used strictly in accordance with this Policy.

CPA reserves the right to monitor the use of its e-mail facilities in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Email Requests for Disclosure of Personal Data

Where possible requests for personal data by third parties should be made in writing on headed paper as a means of verifying that the request is genuine.

Email requests can be accepted on a case-by-case basis as long as you are satisfied the request is genuine. To verify whether a request is genuine, you need to:

- Check the email is a valid address and that it is from an official email account.
- Call the telephone number displayed on the email request to confirm the identity of the person requesting the personal data and that they are from the organisation they claim to be representing.

Once you are satisfied the request is genuine, you may respond by email to the request for personal information.

CCTV
CPA operates close circuit television cameras (CCTV) across its site, for the security and safety of its staff and learners.

CPA is committed to the protection and security of personal data especially as applied in the use, operation and monitoring of CCTV images. As such:

- All security staff involved in the recording, observation and capture of images must act in an ethical and lawful manner in accordance with legislation and must receive adequate training to ensure their understanding of compliance legislation.
- Only authorised persons involved in the monitoring or investigation can view CCTV images.
- All recorded material will be treated as confidential and unless required for evidence.
- CCTV will not be retained for longer than necessary in accordance with the data protection principles.
- Data is stored and managed automatically by the CCTV digital recorders which use software programmed to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces a minimum of 1 month rotation in data retention.

If CCTV images are retained beyond the retention period, they are to be stored in a secure place to which access is controlled and are to be erased when no longer required.

Direct Marketing
The Business Development Manager of CPA's marketing function has responsibility for all outgoing mail or telephone marketing and for CPA's website. No personal data must be used or published in these contexts without the specific approval of the Quality Controller.

Research
Where personal data is collected ONLY for research purposes it is exempt from certain aspects of the Data Protection Act 2018.

However, personal data collected for research purposes must not be used in forming any decisions about a particular individual and must not be used in any way that will, or is likely to, cause distress to any data subject.

If you are collecting personal data for research within these parameters the following exemptions apply:

- Processing the personal data for additional research purposes (within the above parameters) other than those notified to the data subject on collection is permitted.
- Personal data processed only for research purposes (within the parameters) may be kept indefinitely.
- Personal data processed only for research purposes (within the parameters) and which is not made available in any form that identifies data subjects is exempt from the data subject's right of access.

Therefore, it is recommended that when personal data is collected for research purposes:

- The data subject should be informed of the purposes for which the data is being collected.
- Any data collection forms should make clear that the data will be used only for research, what the research is for, and that any published results will be anonymised.

All other provisions of the Act apply, notably the requirement for adequate security when processing personal data whether or not within the above parameters.

Sensitive Personal Data

The Data Protection (Processing of Sensitive Personal Data) Order 2000 allows the processing of sensitive personal data for research purposes where the following conditions are met:

- Data is not used to support measures or decisions about individuals without their explicit consent.
- The processing for research does not cause substantial damage or distress to any person.
- The processing for research purposes is in the substantial public interest.

References

References Provided by CPA

As part of its commitment to fair processing and openness CPA will disclose references provided by CPA to staff upon request. To obtain a copy of the reference a subject access request should be made in accordance with the procedure detailed within this Policy.

Staff are reminded that any reference they provide will be potentially disclosable to the individual by CPA or by the receiving third party. They must exercise due care and skill in providing a reference and ensure the reference is factually correct. Any expression of opinion should be reasonable and must be justified.

References Received by CPA

References received by CPA are not exempt from the right of access, this means that any references received by CPA will be disclosable. Referees from a third party should be informed that CPA's policy is to disclose references in a subject access request. Where the third party has expressed their refusal to give permission for disclosure of the information referees' personal details should be redacted and any other information which could identify them.

Breach of the Policy

Should staff not process data in accordance with this Policy, CPA and the individual in breach could be liable to criminal prosecution and civil claims for damages.

If any member of staff or learner is found to have breached this Policy, it will be considered to be a disciplinary offence. The individual may be suspended from having access to any personal data held by CPA and will be subject to action under CPA's Disciplinary Procedure.

If any staff member or learner believes CPA has infringed her/his rights under this Policy, they should raise this concern under CPA's Grievance or Complaints Procedure respectively.

Any member of staff or learner who considers that the Data Protection Policy is not being followed should raise the matter with the Director.

Skills Funding Agency

CPA is required to provide statistical information on its learners and staff to its funding bodies. The Skills Funding Agency ("SFA").

Data Protection Act 2018 – The information you provide on the enrolment form will be passed to the Skills Funding Agency. The SFA is responsible for funding and planning education and training for over 16-year-olds in England and is registered under the Data Protection Act 1998. The information you provide will be shared with other organisations for the purpose of administration, careers and other guidance and statistical and research purposes. The SFA is also a co-financing organisation and uses European Social Funds from the European Union to directly or indirectly part- finance learning activities, helping develop employment by promoting employability, business spirit and equal opportunities, and investing in human resources. Further information about partner organisations and what they do, may be found at https://www.gov.uk/government/organisations/skills-funding-agency and by following the links to data protection.

At no time will your personal information be passed to organisations for marketing or sales purposes. From time-to-time learners are approached to take part in surveys by mail and phone, which are aimed at enabling the SFA and its partners to monitor performance, improve quality and plan future provision.

SUBJECT ACCESS REQUEST FORM
Staff, Learner & Third Party

Details of the person requesting the information.
Full name ……
Address……
……
Telephone number ……
Email ……

Are you the Data Subject?

Yes if you are the Data Subject please supply evidence of your identity e.g., driving licence birth certificate (or photocopy) and, if necessary, a stamped addressed envelope for returning the document (please go to question 5).

No are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed (please complete questions 3 and 4)

Details of the subject (if different to the person requesting the information).
Full name ……
Address……
……
Telephone number ……
Email ……

Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.
……
……

Please state below specific information or document(s) you wish to see, for example a particular examination report, a specific departmental file etc, please describe these below:
……
……

Office use only Request received: ……
Date completed: ……
Notes ……