ICPA Data Protection Policy

Introduction

ICPA is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal information. The centre needs to collect and use certain types of information about applicants, learners, employees and other individuals (data subjects) who work and study at the Institute or come into contact with it. This information will be obtained for a relevant purpose and will be collected and retained to meet that purpose. It will be dealt with appropriately however it is collected, recorded and used; whether on paper, electronic or recorded on other material and it will be safeguarded to ensure the Institute complies with relevant legislation. The information will not be held longer than is necessary. ICPA regards the lawful and correct treatment of personal information as a priority and therefore it will ensure that this information is treated correctly. The Institute will process and control such information primarily for recruitment, attendance, assessment, certification, personnel, administrative and payroll purposes.

Scope

This policy applies to all stakeholders of ICPA. This policy does not form part of the formal employee contract nor of the learner contract with the Institute, but it is a condition of both that the rules and policies made by the Institute will be complied with. Any failure to comply with this policy will be dealt with in a formal manner.
All employees, learners and other data subjects are entitled to:

- Know what information the centre holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up-to-date
- Know what the centre is doing to comply with its legal obligations

Implementation of the Policy –

Data Security

All employees are responsible for ensuring that:

- Any personal data which they hold is kept and disposed of securely
- Personal information is not disclosed either orally, in writing or accidently or otherwise to any unauthorised third party

Employees should note that unauthorised disclosure will usually be dealt with formally. Personal information must be:

- Kept in a locked office, filing cabinet or drawer
- Password protected when stored on a computer
- Secure if it is held on a portable device

Unauthorised Access

- Any employee or learner who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party will be dealt with formally in accordance with Institute's procedures.

Learner Obligations

Learners must ensure that all personal data provided to the Institute is accurate and up-to-date.

Rights of Access to Information

Employees, learners and other data subjects have the right of access to any personal data that is being kept about them either electronically or in other files.

Certain disclosures may be made without consent so long as the information is requested by an appropriate Government or regulatory authority for one or more of the following purposes (requests must be supported by appropriate paperwork):

• To safeguard national security
• Prevention or detection of crime including the apprehension or prosecution of offenders
• Assessment or collection of tax duty
• Discharge of regulatory functions (includes health, safety and welfare of persons at work)
• To prevent serious harm to a third party
• To protect the vital interests of the individual, this refers to life and death situations

Retention of data

ICPA will not hold data longer than is necessary. Information about learners will be retained for 4 years after the date when they leave the Institute. This will include the results of the qualifications studied and any references provided. Information about staff will be retained for at least six years after they leave the Institute. However, some information will be held for a longer period, for example data which relates to tax or pensions and any references provided.

Conclusion

Any stakeholders who wish to clarify the contents of this policy should speak to staff in our support executive. Any employees or learners who consider that this policy has not been followed in respect of personal data about themselves or about other data subjects should raise the matter using the Institute's formal complaints procedure.