ICMG Ltd
Data Protection Policy, Procedure and Guidelines

POLICY REVIEWS:

Review Date	Review By

1. POLICY STATEMENT

In order to properly carry out its business, the company needs to hold certain information about its employees, learners and other users. It is also necessary to process information so that staff can be recruited and paid, courses organised and the legal obligations to funding bodies, Government agencies and others met. To comply with the law, information will be collected and used fairly, stored safely and not disclosed to any person unlawfully.

2. DEFINITIONS

'Data Protection' is used to describe a set of statutory rules which aim to ensure, firstly, that organisations and individuals who collect, store or use information about other individuals who are still living, do not abuse the information; and, secondly, that the people about whom information is collected and used, know of its existence and know how to correct it if it is wrong.

'The Data Protection Act 1998' outlines the principles of data protection and gives a legal obligation on all data users to comply with those principals. Data protection law is enforced in the UK by the **Information Commissioner's Office (ICO)**.

A **'Data Subject'** is any individual about whom personal data is kept. This will include: employees; past employees; learners and other customers; job applicants; prospective customers (e.g. a marketing database); agency staff; contractors; suppliers.

An **'Adult'** is defined by law as any person aged 18 years or older.

'Personal data' is any information that the Company holds and/or uses on Data Subjects (staff or learners). This will include name and address; date of birth; telephone numbers; email or social networking contact details; learner academic progress and achievements; financial information including salaries; next of kin details; appraisal, disciplinary and annual leave details; sickness and medical records; previous employment history, qualifications and skills.

'Sensitive data' is information regarding the Data Subject's physical or mental health; sexual activities; political or religious views; trade union membership; ethnicity or race.

'Data Processing' is any use to which personal data are put, including: obtaining and retrieving; holding and storing; making available to others within or outside of the Company (including by email); printing, sorting, comparing or destroying.

The **'Data Controller'** is the Company that determines how personal data will be used. The **'Data Protection Officer'** is the Managing Director of the company and the main contact for all data compliance issues.

3. PRINCIPLES

This Policy confirms compliance with, and guidance, about, the Data Protection Act 1998 (subsequently referred to as the 1998 Act), including any updates or amendments and all Codes of Practice.

All staff, learners and other Data Subjects are entitled to:

- Know what information the company 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 Company is doing to comply with its obligations under the 1998 Act

4. SCOPE AND LIMITATIONS

The Company and all staff or others who process or use any personal information must ensure that they follow the requirements of the 1998 Act at all times.

5. RESPONSIBILITIES

The Managing Director: The Archive, Information and Records Officer is the central point of contact for advice and day-to-day guidance on data compliance issues.

All staff are responsible for complying with the 1988 Act when collecting information about other people (e.g. about learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances).

All staff are responsible for ensuring that any personal data which they hold is kept securely, and that personal data is not disclosed either orally or in writing to any unauthorised third party.

All staff are responsible for checking that any information they provide to the Company in connection with their employment is accurate and up to date.

All learners are responsible for ensuring that any personal data provided to the Company is accurate and up to date.

Any breach of this Policy will lead to disciplinary action being taken, or access to Company facilities being withdrawn, or even a criminal prosecution.

6. IMPLEMENTATION ARRANGEMENTS

Storage and handling of personal data

The Company will ensure that any personal data is kept securely. This will be in locked filing cabinets or drawers; be password protected or encrypted if held electronically; or kept secure if stored on any other medium.

The Company will provide a central facility for the secure, managed archiving of personal (and other) data which is not required for immediate access. Some data may be scanned and held electronically, where appropriate

The risks of holding data on portable devices, including laptops, memory sticks and mobile phones, will be recognised and all reasonable safeguards taken against loss or unauthorised access.

Where it is essential to post confidential documents then an appropriate service, such as the Royal Mail Special Delivery or another reputable courier service, should be used.

If confidential be in a sealed envelope and marked 'Confidential', with the addressee clearly shown.

Voicemail messages and Automatic Replies to emails should not include any information which is confidential and should not provide details regarding the period or nature of the

voicemail user's absence (e.g. on annual leave).

Care must be taken when sending faxes to ensure that the recipient's number is correct, in service and that the recipient is available to receive, and confirm receipt of, the fax. Only essential personal data should be included in that fax. All documents and faxes should be removed from the fax machine.

When photocopying, care should be taken to ensure that original documents and any copies of them are removed from the machine.

When disposing of any records which hold personal data, action will be taken to ensure that it is securely and permanently destroyed

When disposing of any portable devices which hold personal data, action will be taken to ensure that all data is permanently erased or destroyed.

Access to personal data

The Company will clearly indicate to all staff and learners the type of data it holds and processes about them, and the reasons for which it is processed. The company will also clearly indicate to all staff and learners how they may access the relevant data it holds.

The Company will ensure that any staff, learner or other Data Subject has the right to access any personal data (paper or electronic) that is being kept about them. Any request for access will be in writing (or by email), or through a company Access to Data form, and will receive a prompt response, and always within 40 days of that request being received.

Requests for personal data should normally be received in writing (including fax or email). When a telephoned request is received, an identity check should be conducted before disclosing personal information. Wherever possible, telephone conversations covering confidential information should take place in areas where the risk of being overheard is minimised.

In most cases the Company can only process or share personal data with the consent of the Data Subject. In some cases, if the data is sensitive (i.e. concerning physical or mental health, sexual activities, political or religious views, trade union membership, or ethnicity or race), consent specific to that data must be obtained. However, agreement to the

Company processing some specified classes of personal data (e.g. ethnicity data) is a condition of acceptance of a student onto any course, and a condition of employment for staff. A declaration giving consent to process those specified types of information will be signed by students when enrolment takes place and by prospective staff when an offer of employment is made.

Where learners are attending company under sponsorship agreements (e.g. with employers), routine reports on academic progress and attendance will be provided to those sponsors.

Under the 1998 Act, all company learners are considered to be mature enough to understand their rights as a Data Subject and to request access to their personal information. The rights and views of all company learners will therefore be considered when handling, storing or sharing their personal data.

7. MONITORING AND REVIEW

The Data Protection Policy will be reviewed on an annual basis.

Any initial questions or concerns about the interpretation or operation of this policy should be raised with the Company Managing Director.

8. SUPPORTING/RELATED DOCUMENTS

www.ico.gov.uk/for_organisations/data_protection.aspx
For practical and legal guidance on all aspects of data protection, including the use of CCTV

www.jisclegal.ac.uk
For legal advice relating to the use of ICT-related data in education, Includes clear guidance regarding procedures on dealing with police requests for access to personal data (enter 'Police' in search box).

PROCEDURE

In summary, the 1998 Act states that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for specified and lawful purposes, and shall not be processed in any manner incompatible with those purposes
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not be kept for longer than is necessary for those purposes
- Be processed in accordance with the Data Subject's rights
- Be kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to a country outside the European Economic Community, unless that country has equivalent levels of protection for personal data

GUIDELINES

The information that staff will deal with on a day-to-day basis will be 'standard' and will cover categories such as:

- General personal details, such as name and address
- Details about class attendance, course work marks and grades, and associated comments
- Notes of personal supervision, including matters about behaviour and discipline

The Company will ensure through enrolment procedures, that all learners give their consent to this sort of processing, and are notified of their rights, as required by the 1988 Act, as part of the recruitment and/or induction process.

'Sensitive' information about a Data Subject's physical or mental health; sexual activities; political or religious views; trade union membership; or ethnicity or race, will only be collected and processed with the subject's specific consent, or where required by agreed enrolment

procedures.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in this Data Protection Policy. In particular, staff must ensure that records are:

- Accurate
- Up-to-date
- Fair
- Kept and disposed of safely, and in accordance with the Company policy

Staff must not disclose personal data to any other person (unless it is for accepted academic or pastoral purposes) without authorisation or agreement from the appropriate Data Processor.

Staff shall not disclose personal data to any other staff member, except with the authorisation or agreement of the Managaging Director, or in line with Company policy.

Staff should be aware of, and comply with, the principles regarding records management and data retention, as set out in the Records Management and Archiving Policy.

Before processing any personal data, all staff should consider the following checklist:

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the Data Subject's specific consent?
- Has the Data Subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the Data Subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the Data Subject's consent to process, are you satisfied that it is in the best interests of the Data Subject to collect and retain the data?

Remember: data includes hand-written notes as well as more formal word-processed and digitally stored records.