Data Protection Policy

1. Introduction
   This policy and procedure apply to all JPIE employees, Academic Council members, Exam Board members, JPIE associates, and any other person with access to personal or sensitive information processed by JPIE.

   The policy covers obtaining personal data, its storage and security, its use and its ultimate deletion or disposal.

   Everyone managing and handling personal information must understand their responsibilities in complying with the Data Protection Act.

   This procedure takes effect from October 2022 and supersedes all previous policies.

2. Data Protection Act
   JPIE must comply with the Data Protection Act and process all personal information in accordance with the Data Protection Principles. The Data Protection Act 1998 came fully into force on 1st March 2000. It outlines eight Data Protection Principles which must be complied with when collecting and holding personal data.

3. Principles of Data Protection
   a. Principle 1 – Personal data shall be published fairly and lawfully.
   b. Principle 2 – Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or those purposes.
   c. Principle 3 – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
   d. Principle 4 – Personal data shall be accurate and, where necessary, kept up to date.
   e. Principle 5 – Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.
   f. Principle 6 – Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
   g. Principle 7 – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.
   h. Principle 8 – Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

   JPIE employees or others who process or use personal information for JPIE must ensure that they always follow these principles.

4. Processing personal data

   The definition of processing in relation to data protection is very wide. Obtaining, holding, filing, organising, transmitting, retrieving, disseminating, disclosing and destroying data are all deemed to be processing in addition to any other process carried out on the data.

   a. JPIE employees and others acting on behalf of the JPIE must only have access to personal data necessary to carry out their duties and responsibilities.
   b. All forms used to obtain personal data, such as application forms or registration forms, must:
      - State the purpose/s for which the information is required
      - Be reviewed regularly to check that all of the information asked for is still required and necessary.
      - Be checked for the accuracy of the data before they are used for any processing. If in doubt about the accuracy of the data, they should be referred back to the data subject for confirmation
   c. Personal data must be collected and handled in a way that complies with the Act and meets the eight principles above. This imposes a duty on JPIE to ensure that individuals are made aware of the uses that will be made of the information that they supply and give their consent to this.
   d. If an outside agency provides data, the agency must be asked to confirm in writing that the data were obtained fairly and lawfully, in compliance with the Act.
   e. Any information regarding criminal convictions must be treated as sensitive information and handled accordingly. Any request made by the JPIE for such information must be fully justified. Advice should be sought from the Data Protection Officer.
   f. Where personal data are provided for the purpose of placing a contract to which the data subject is a party, then such data is considered to be fairly and lawfully obtained.

   JPIE must ensure that necessary and sufficient precautions are in place to prevent misuse or unauthorised access to data and have security measures in place to prevent loss or damage to data.

   a. Filing cabinets containing personal data must be locked outside of regular working hours, and keys must be held securely by nominated staff.
   b. Electronic files must be password protected, and passwords must be changed regularly.
   c. All such electronic data must be stored in secure server areas, not on computer hard drives, laptops or other mobile devices.
   d. Any electronic data backed up to media, such as a memory stick or external hard drive, must be kept physically secure.
   e. If any data are to be taken from the office (e.g. to work at home), then the data must be held securely at all times, whilst in transit and at the location they are being held.
   f. Where external bodies process or hold any of the JPIE's personal data, then JPIE must be satisfied that the data is stored securely and with due regard to the obligations of the Act.

5. Contact details, including email

   JPIE will keep a record of contact details, including Email addresses, to enable us to contact staff members and students on JPIE-related matters. We will not give Email addresses to any unauthorised third parties.

6. Uses of information

   JPIE collects and processes information about students for various registration, membership, assessment, research, administrative and management purposes. JPIE will securely hold student personal information, both in hard copy format and electronically, and under the Data Protection Act 1998 (DPA) requirements.

   JPIE may share student information with third parties where obliged or allowed to do so by law (for example, for statutory returns, to work with partner colleges, or to enable online services to students).

   JPIE will send some of the student information it holds to Ofqual. Student contact details do not form part of the Ofqual student record. Ofqual collects and is responsible for the database in which it stores the JPIE student record. For example, Ofqual uses this information in its own right to publish statistics about students in higher education.