Data Protection Policy

Statement of purpose

ISP is registered on the Data Protection register as a statutory requirement for organisations that hold personal data.

The registration period is 12 months and therefore renewal is annually.

Scope

This policy applies to all staff, employees, part time employees, learners, EPA candidates and Provider personnel. ISP will ensure that it informs everyone about data protection and GDPR issues and their rights to access and limit access to their own personal data. ISP holds personal data and will ensure compliance with the Data Protection Act 1998 and GDPR.

Data Protection Act and GDPR

The Data Protection Act 1998 and subsequent GDPR updates protects employees, etc against the misuse of personal data, and covers both manual and electronic records.

The Act and GDPR requires that any personal data held should be:

- processed fairly, lawfully and not be misused;
- obtained and processed only for specified and lawful purposes;
- adequate, relevant and not excessive;
- accurate and kept up to date;
- held securely and for no longer than is necessary; and
- Not transferred to a country outside the European Economic Area unless there is an adequate level of data protection in that country.
- Processed in accordance with the Data subject's permission
- The responsibility of the data controller and data processor to be processed appropriately

If employees, etc access another employee's or learner's records without authority this will be treated as gross misconduct and is a criminal offence under the Data Protection Act 1998, section 55.

Purposes for which personal data may be held (learners, EPA candidates, ATOs)

With data subject's permission, employees of ISP may access information about learners, EPA candidates and Providers for the following purposes:

- To maintain or process records
- To process data for certification
- To help improve our service to learners

From time to time, employees of ISP may send out information to learners about new products or other information that may be of interest to learners. Data subjects need to subscribe to this process to receive this information, see mailing list at eqa@the-isp.org

Transfer of data

Certain personal information may be transferred or made available to:

- Other third parties who audit systems and information to fulfil legal requirements
- Government organisations / statutory bodies to fulfil regulatory requirements
- Other third-party contractors and suppliers to ISP for the purposes of storing information, processing requests or arranging delivery of the product or service you have requested, with data subject's permission.

We will not disclose, rent, sell or otherwise transfer your personal information without your consent other than the criteria set out above.

All of our data controllers, data processors, service providers and contractors are required to maintain the confidentiality and security of your personal information and to use it only in compliance with applicable data privacy laws, GDPR and are prohibited from using or disclosing your personal information for any purpose other than providing the services on our behalf or as otherwise required by applicable law.

Purposes for which personal data may be held (employees)

Personal data relating to employees may be collected primarily for the purposes of:

- recruitment, promotion, training, redeployment, and/or career development;
- administration and payment of wages and sick pay;
- calculation of certain benefits including pensions;
- disciplinary or performance management purposes;
- performance review;
- recording of communication with employees/students and their representatives;
- compliance with legislation;
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and

- Staff, volunteers and students, staffing levels and career planning.

ISP considers that the following personal data falls within the categories set out above:

- Personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant;
- references and CVs;
- emergency contact details;
- notes on discussions between management and the employee/student;
- appraisals and documents relating to grievance, discipline, promotion, demotion, or termination of employment;
- training and certification records;
- salary, benefits and bank/building society details; and
- Absence and sickness information.

Employees, potential employees, volunteers and students will be advised of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed in accordance with GDPR. ISP will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

Sensitive personal data

Sensitive personal data includes information relating to the following matters:

- the employee's/student's racial or ethnic origin;
- his or her political opinions;
- his or her religious or similar beliefs;
- his or her trade union membership;
- his or her physical or mental health or condition;
- his or her sexual orientation; or
- The commission or alleged commission of any offence by the employee/student.

Responsibility for the processing of personal data

ISP's Data Controller is the Managing Director who is responsible for ensuring all personal data is controlled in compliance with the Data Protection Act 1998 and GDPR. Data Processors are our employees and assessment associates, who are also responsible for ensuring all personal data is processed in compliance with the Data Protection Act 1998 and GDPR.

Employees, EPA candidates and students who have access to personal data must comply with this Policy and adhere to the procedures laid down by the Data Controller. Failure to comply with the Policy and procedures may result in disciplinary action up to and including summary dismissal.

Use of personal data

To ensure compliance with the Data Protection Act 1998, GDPR and in the interests of privacy, employee/student confidence and good employee/student relations, the disclosure and use of information held by ISP is governed by the following conditions:

- personal data must only be used for one or more of the purposes specified in this Policy;
- Documents may only be used in accordance with the statement within each document stating its intended use; and
- provided that the identification of the individual employees/students is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data (e.g., surveys, staff, volunteers and students, staffing level figures); and
- Personal data must not be disclosed, either within or outside ISP, to any unauthorised recipient.

Personal data held for equal opportunities monitoring purposes

Where personal data obtained about candidates is to be held for the purpose of Equal Opportunities monitoring, all such data must be made anonymous.

Disclosure of personal data

Personal data may only be disclosed outside ISP with the data subject/employee's/student's written consent, where disclosure is required by law or where there is immediate danger to the employee's/student's health.

Accuracy of personal data

ISP will review personal data regularly to ensure that it is accurate, relevant and up to date. In order to ensure that our files are accurate and up to date, and so that ISP is able to contact the data subject/employee/student or, in the case of an emergency, another designated person, employees/students must notify their line manager or the Chief Executive as soon as possible of any change in their personal details (e.g., change of name, address; telephone number; loss of driving license where relevant; next of kin details, etc).

Access to personal data ("Subject Access Requests")

Data Subjects/Employees/Students have the right to access personal data held about them. The Company will arrange for the data subject/employee/student to see or hear all personal data held about them within 21 days of receipt of a written request.

Retention of records.

ISP follows the retention periods recommended by the Information Commissioner in its Employment Practices Data Protection Code and GDPR requirements.

These are as follows, in the absence of a specific business case supporting a longer period.

Document	Retention period
Application form	Duration of employment
References received	1 year
Payroll and tax information	6 years
Sickness records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment

References given/information to enable references to be provided	5 years from reference/end of employment
Summary of record of service, eg name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years

Any data protection queries should be addressed to the ISP Data Protection/GDPR Officer.