Data Protection Policy

(v1.72 06/23)

1 Introduction

1.1 The policy is subject to regular review to reflect, for example, changes to legislation or to the structure or policies of the Information Commissioner's Office (ICO) or other relevant regulatory authority. All our staff are expected to apply the policy and to seek advice when required.

1.2 We need to collect and use certain types of information about people with whom we deal in order to operate at full potential. The personal information we collect must be dealt with properly however it is collected, recorded and used – whether on paper, electronically, or other.

1.3 We regard the lawful and correct treatment of your personal information as important to the achievement of our objectives, the success of our operations, and to maintaining confidence and strong business partnerships with you our customers. We therefore need to ensure that we treat personal information in full compliance with the General Data Protection Regulation and any national law applicable to our business.

2 Principles

2.1 The eight fundamental Principles required in the protection of personal information are set out by the legislation are:
2.1.1 Personal data shall be processed fairly, lawfully and transparently;
2.1.2 Personal data shall be collected for specified, explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
2.1.3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed;
2.1.4 Personal data shall be accurate and, where necessary, kept up-to-date;
2.1.5 Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose or those purposes for which is it processed;
2.1.6 Personal data shall be processed in accordance with the rights of data subjects under applicable laws;
2.1.7 Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage using appropriate technical or organisational measures;
2.1.8 Personal data shall not be transferred to an organisation in a country or territory outside the European Economic Area unless (i) 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; (ii) we use specific contracts approved by the European Commission which give personal data the same protection it has in Europe; and/or (iii) if the organisation is based in the US and they are part of the Privacy Shield..

2.2 Through appropriate management and strict application of criteria and controls we will do above and beyond the requirements of the legislation to protect your personal information. How we will do this is firstly by complying with the above principles but above the requirements of the legislation, Upskill People conduct procedural steps known as a Privacy Impact Risk Assessment (PIRA) on all of our online learning platforms. This process helps assess privacy risks to individuals in the collection, use and disclosure of information. PIRAs help identify privacy risks, foresee problems and bring forward solutions when handling personal information. The PIRA will be reviewed once every 12 months or as required to ascertain that it is still relevant and compliant.

2.3 We (the Supplier) abide by the following principles when handling your personal information and the protection of data;
2.3.1 to observe fully conditions regarding the fair collection and use of information;
2.3.2 to meet the legal obligations to specify the purposes for which information is used;
2.3.3 to collect and process appropriate information only to the extent that it is needed to for fill our operational needs or to comply with any legal requirements;
2.3.4 to ensure the quality of information used;
2.3.5 to ensure that the information is held for no longer than is necessary;
2.3.6 to ensure that the rights of people about whom information is held can be fully exercised under the Act (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information);
2.3.7 to take appropriate technical and organisational security measures to safeguard personal information;
2.3.8 to ensure that personal information is not transferred abroad without suitable safeguards.

2.4 To assist in achieving compliance with these principles, we have;
2.4.1 appointed a Data Protection Officer with specific responsibility for data protection within our company;
2.4.2 created a dedicated Information Access Team to assist all our staff in understanding and applying the data protection principles and to liaise with external parties.

3 Retention

3.1 We retain personal data within our business systems in accordance with applicable laws. This means for our business that, for employees, we will retain personal data for up to 6 years after the employment has terminated. We shall

retain personal data of our clients' employees in accordance with our contract with the client and the client's instructions, subject to any other legal, tax or accounting requirements.

4 Data Protection Promise

We (the Supplier) promise to:

4.1 value the personal information entrusted to us and make sure we respect that trust;

4.2 go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;

4.3 consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;

4.4 be open with individuals about how we use their information and who we give it to;

4.5 make it easy for individuals to access and correct their personal information;

4.6 keep personal information to the minimum necessary and delete it when we no longer need it;

4.7 have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;

4.8 provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or fail to look after personal information properly;

4.9 put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and

4.10 regularly check that we are living up to our promises and report on how we are doing.

END