Data Protection Policy

Introduction

1.1 CT Skills is committed to being transparent about how it collects and uses the personal data of its learners, staff, and others, and to meeting data protection obligations, in accordance with the General Data Protection Regulations (GDPR) May 2018 and Data Protection Act 2018. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 This policy applies to all personal data processed for HR-related and business purposes such as, but not limited to the personal data of learners, parents and guardians, job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees.

1.3 CT Skills Limited of Priory Court, Beeston, Nottingham NG9 2TA is registered with the Information Commissioners Officer as the Data Controller and Data Processer. Registration Number: Z8790632

1.4 The organisation has appointed the Data Protection Officer at a Company level. Questions about this policy, or requests for further information, should be directed to admin@ctskills.co.uk.

Definitions

1.5 *"Personal Data"* is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

1.6 *"Special categories of personal data"* means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

1.7 *"Criminal records data"* means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Principles

1.8 CT Skills processes personal data in accordance with the following data protection principles:

(a) The organisation processes personal data lawfully, fairly and in a transparent manner.

(b) The organisation collects personal data only for specified, explicit and legitimate purpose.

(c) The organisation processes personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.

(d) The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

(e) The organisation keeps personal data only for the period necessary for processing.

(f) The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

1.9 The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

1.10 Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done so only when conditions meet Article 9 of the GDPR Act or explicit consent is given.

1.11 The organisation will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

1.12 Personal data gathered during the learner, employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's learner record, personnel file (in hard copy or electronic format, or both), and on internal learner systems and HR systems. The periods for which the organisation holds personal data are contained in its privacy notices to individuals.

1.13 The organisation keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR) May 2018.

Individual rights

1.14 As a data subject, individuals have several rights in relation to their personal data.

Subject access requests

1.15 Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

(a) whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.

(b) to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.

(c) for how long his/her personal data is stored (or how that period is decided).

(d) his/her rights to rectification or erasure of data, or to restrict or object to processing.

(e) his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and

(f) whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

1.16 The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless he/she agrees otherwise.

1.17 If the individual wants additional copies, the organisation may charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

1.18 To make a subject access request, the individual should send the request to admin@ctskills.co.uk or complete the form available on cloud. In some cases, the organisation may need to ask for proof

of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

1.19 The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

1.20 If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

Other rights

1.21 You have several other rights in relation to your personal data. You can require CT Skills to:

(a) rectify inaccurate data.

(b) stop processing or erase data that is no longer necessary for the purposes of processing.

(c) stop processing or erase data if your interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data).

(d) stop processing or erase date if processing is unlawful; and

(e) stop processing data for a period if data is inaccurate or if there is a dispute about whether your individual interests override the organisation's legitimate grounds for processing data.

(f) Limit the extent of the processing of your personal data according to your wishes.

(g) Not be subject to decisions using automated decision making or profiling

1.22 To ask the organisation to take any of these steps, you should send the request to admin@ctskills.co.uk.

Data security

1.23 CT Skills takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

1.24 This policy also applies to staff and students who process personal data "off-site", e.g., when working from home, and in circumstances additional care must be taken regarding the security of data.

1.25 Where CT Skills engages third parties to process personal data on its behalf, such parties do so based on written instructions, under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

1.26 Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

1.27 If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

1.28 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

1.29 The organisation will not transfer personal data to countries outside the EEA without explicit consent of the individual.

Individual responsibilities

1.30 Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.

1.31 Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship, or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.

1.32 Individuals who have access to personal data are required:

(a) to access only data that they have authority to access and only for authorised purposes.

(b) not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation.

(c) to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).

(d) not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the date and the device; and

(e) not to store personal data on local drives or on personal devices that are used for work purposes.

1.33 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy,

such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

1.34 The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Compliance

1.35 This policy applies to all staff and learners of CT Skills. Any breach of this policy will be dealt with under the Disciplinary procedure.

1.36 Other agencies (sub-contractors for example) and individuals working with CT Skills and who have access to personal information will be expected to read and comply with this policy. Such bodies will sign a contract which among other things will include an agreement to abide by this policy.

1.37 This policy will be reviewed at least annually and will reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

Authorised: **Alex Ford (Chief Executive Officer).**

Date: 30.07.2021