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 UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018 and Data (Use and Access) Act 2025. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 CT Skills is responsible for demonstrating compliance with applicable data protection legislation. The organisation maintains appropriate policies, procedures, records of processing activities, staff training arrangements and monitoring processes to evidence compliance.

1.3 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.

1.4 CT Skills Limited of Charlotte House Stanier Way, The Wyvern Business Park, Derby, DE21 6BF is registered with the Information Commissioner's Office (ICO) as a Data Controller. Registration Number: Z8790632

1.5 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.

1.6 The organisation will only process personal data where a lawful basis exists under Article 6 UK GDPR, including consent, contract, legal obligation, vital interests, public task or legitimate interests, as applicable.

Definitions

1.7 *"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.

1.8 *"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.

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

Data Protection Principles

1.10 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 purposes.

(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.

(g) The organisation will maintain records of processing activities and make them available to regulators where required by law.

(h) The organisation will maintain appropriate privacy notices to inform individuals how their personal data is collected, used, shared, retained and protected.

(i) The organisation may process personal data on the basis of recognised legitimate interests where permitted by law and where such processing is necessary for purposes identified within applicable data protection legislation.

1.11 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.

1.12 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 under Article 9 UK GDPR are met, or explicit consent is given.

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

1.14 Personal data gathered during the learner, employment, worker, contractor or volunteer relationship, or apprenticeship 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.

1.15 Personal data will be retained in accordance with the organisation's Data Retention Schedule. Records will be securely deleted, anonymised or destroyed once they are no longer required for a lawful business purpose or legal obligation.

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

Individual rights

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

Subject access requests

1.18 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 UK and/or countries not subject to a UK adequacy decision 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.

1.19 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.

1.20 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.

1.21 To make a subject access request, the individual should send the request to admin@ctskills.co.uk 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.

1.22 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.

1.23 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

1.24 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 data 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) Provide information about significant decisions made using automated processing, request human review, express their views, and challenge such decisions where applicable.

CT Skills will ensure that any significant automated decision-making is subject to appropriate safeguards, human oversight and transparency measures in accordance with applicable legislation.

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

Data security

1.26 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.

1.27 The organisation implements appropriate technical and organisational security measures, including user access controls, role-based permissions, secure backups, multi-factor authentication where available, encryption of data and devices where appropriate, anti-malware protection, and regular cyber security awareness training. These measures are reviewed periodically to maintain their effectiveness.

1.28 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.

1.29 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.

Third-Party Processor Due Diligence

1.30 Prior to engaging any third-party processor or cloud service provider, CT Skills will undertake appropriate due diligence to assess the provider's ability to meet data protection, confidentiality and information security obligations. The organisation will maintain appropriate contractual arrangements and periodically review provider compliance and security controls.

Impact assessments

1.31 Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individuals' 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 Protection by Design and by Default

1.32 CT Skills will consider data protection requirements at the earliest stage of any new project, system, process or activity involving personal data. Appropriate technical and organisational measures will be implemented to ensure that only the personal data necessary for each specific purpose is processed and that privacy risks are identified and managed from the outset. The organisation will consider whether a Data Protection Impact Assessment (DPIA) is required where processing is likely to result in a high risk to the rights and freedoms of individuals.

Artificial Intelligence and Emerging Technologies

1.33 Where artificial intelligence, machine learning, analytics tools or other emerging technologies are used to process personal data, CT Skills will ensure that appropriate risk assessments, transparency measures and safeguards are implemented to protect the rights and freedoms of individuals.

Children's Personal Data

1.34 Where personal data relating to children or young people is processed, CT Skills will give particular consideration to the child's best interests, age, level of understanding and vulnerability when designing services, communications and processing activities.

Data breaches

1.35 If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals. Where required by law, the organisation will notify the Information Commissioner's Office within 72 hours of becoming aware of a personal data breach.

1.36 The organisation will record all data breaches regardless of their effect.

1.37 All staff, contractors and learners must report any actual or suspected personal data breach immediately via the organisation's incident reporting procedures.

1.38 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

1.39 The organisation will only transfer personal data outside the United Kingdom where appropriate safeguards are in place in accordance with UK GDPR and applicable data protection legislation.

1.40 Such safeguards may include adequacy regulations, the International Data Transfer Agreement (IDTA), approved contractual clauses, or other lawful transfer mechanisms recognised under UK law.

Individual responsibilities

1.41 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.

1.42 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.

1.43 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 data and the device; and

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

1.44 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.

Data Protection Complaints

1.45 CT Skills has established a process for receiving, investigating and responding to data protection complaints from data subjects.

1.46 Individuals who have concerns regarding the processing of their personal data should submit their complaint to the Data Protection Officer by emailing admin@ctskills.co.uk.

1.47 Complaints will be acknowledged promptly and investigated impartially. The organisation will respond within a reasonable timescale and inform the individual of any actions taken.

1.48 If the individual remains dissatisfied, they may raise the matter with the Information Commissioner's Office (ICO).

Training

1.49 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

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

1.51 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.

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 UK GDPR and other relevant legislation.

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

Date: 31st July 2026