Data Protection Policy

September 2025

Version 16

Contents

1. Introduction

This document sets out how VTCT establishes, manages and implements its internal system of controls to meet the requirements of the UK Data Protection Act 2018 incorporating the UK General Data Protection Regulations (UK GDPR) and associated measures to uphold the rights and freedoms of individuals in relation to processing of their personal data.

Data protection compliance and the appropriate and proportionate use of personal data is important to VTCT. Everyone has rights regarding the way in which their personal data is used and VTCT is fully committed to maintaining those rights and for complying with the associated legislation.

VTCT is accountable for maintaining governance and compliance over its processing of personal data and has chosen to adopt recognised privacy and security standards of best practice (ISO 27001) as a means of formally demonstrating accountability and governance and to put compliance at the heart of VTCT's business processes wherever appropriate.

2. Scope

This Policy and any other associated documents form part of VTCT's Information Security Management System (ISMS) framework and set out the basis on which VTCT will process any personal data which the organisation collects directly from individuals (known as 'data subjects') or personal data entrusted to VTCT by other sources.

The purpose of this Policy is to ensure that everyone whose role requires them to access, use, process and/or be responsible for personal data understands those responsibilities and demonstrate good data protection practice.

Additionally, acknowledging that VTCT staff are data subjects too, this document also sets out what VTCT does with staff personal data and the relevant data subject rights.

2.1. Personal Data

Personal Data as defined under UK GDPR is any information which are related to an identified or identifiable natural person. The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data.

2.2. Special Category Data

In addition to general personal data, one must consider above all the special categories of personal data (also known as sensitive personal data) which are highly relevant because they are subject to a higher level of protection. These data include genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.

It is the policy of VTCT that during its acquisition or development of software, systems, equipment and services which support its information assets, they must be risk assessed and, if used for the processing of personal data, subject to a Privacy Impact Assessment (PIA) resulting in appropriate information security requirements or controls being determined and implemented.

3. Principles

VTCT must meet its obligations to ensure that all personal data (including the personal data relating to its staff) is managed fairly, lawfully, accurately and securely. The processing of personal data must be aligned with the following fundamental principles:

Personal data must be processed *lawfully, fairly* and in a *transparent* manner ('lawfulness, fairness and transparency'). Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
What this means for VTCT in practice:
Fairness and transparency: This requires VTCT inform data subjects about why and how VTCT will use their personal data. VTCT must inform its staff, Centre staff, learners and suppliers about the purposes which VTCT will use their data and who else might have access to it. Lawfulness: VTCT must always have a legal justification for using personal data in the way is needed which may require careful analysis on a case-by-case basis. It is very important that data collected for a particular business reason is only used for that purpose as VTCT may not have a legal justification to use it for any other purpose. Sometimes VTCT may be required to obtain consent from individuals for certain types of processing. For example, processing sensitive (also referred to as 'special category') data relating to learners will often require explicit consent and some types of marketing also requires consent. Staff must only use or access personal data where this is needed for the normal performance of a job role. This is especially important when using someone's data in a way that might not be obvious to (or expected by) the individual as this is likely to breach data protection law or infringe data subject rights. Staff must contact VTCT's Data Protection Officer (DPO), or the Information Security Officer (ISO) if they are unsure. In addition, if staff want to use a new software application or have

identified a new supplier or business purpose for processing personal data, they must first engage with key stakeholders to manage any risks involved and ensure that VTCT can use the data in a way that protects the rights of the individuals concerned.
Personal data must be *accurate* and where necessary, kept *up to date* ('accuracy').
What this means for VTCT in practice:
VTCT is required to implement processes and policies to ensure the 'quality' of personal data and make sure that it can be kept up to date and accurate. Although this is ultimately a VTCT responsibility, VTCT will often be reliant on data subjects themselves to tell us of changes to their personal data. From a practical perspective it is often useful to encourage data subjects to contact us if personal data VTCT hold about them becomes out of date or if they are aware of any inaccurate data VTCT hold about them. If a data subject informs VTCT that their personal data are incorrect, or if their circumstances have changed, VTCT must ensure that its records for that individual are promptly updated, including any associated data sets and records. Appropriate policies and processes must be followed (e.g. to periodically review, cleanse and validate existing data sets). Caution must also be exercised when correcting alleged inaccurate personal data records as VTCT must take steps to ensure that there are no accuracy disputes involved.
Personal data must not be kept for longer than is necessary for the purpose or purposes that VTCT requires it ('storage limitation').
What this means for VTCT in practice:
VTCT must not keep personal data in an identifiable form for longer than necessary. If personal data is no longer required for the purposes for which it was collected, it must be securely deleted beyond any ability to re-identify the individuals concerned or securely destroyed. Equipment that has been used to process VTCT personal and business data must be returned to the IT department for secure cleansing prior to re-issue or destruction. Personal data must not be retained 'just in case' it might be useful later. If it is no longer required for the original business purpose it must be deleted in accordance with the retention period for the prescribed information asset. The organisation adopts a default retention period of 6 years plus the current year unless other prescribed by law or statutes. As an Awarding Body, learner achievement data is held for 65 years. Retention periods for information assets are recorded in the Data Retention Schedule. If staff wish to retain personal data for longer than the stated periods, this may be possible but will require the approval of the DPO who may need to identify new legal justification for doing so.
Personal data must be processed in a manner that ensures appropriate security is applied to protect the data, including protection from unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical and organisational security measures.

What this means for VTCT in practice:
VTCT must implement policies and processes to ensure that all personal data is kept secure and confidential and that access to it is only granted to those who have a need to access it. VTCT has invested in the implementation of internationally recognised standards of best practice in the management of information security. Staff must comply with all information security policies, and both demonstrate and encourage positive security behaviour and the secure handling of personal data. Wherever VTCT shares personal data with regulators, service providers or suppliers, VTCT must ensure that the security of personal data is factored in at the earliest stage of negotiating the relationship and that VTCT build appropriate protections for the data into VTCT's contracts with these third parties. Staff are reminded that personal data must be handled in a secure and confidential manner. Contracts of employment or service agreements also contains general confidentiality obligations. Personal data must only be shared or disclosed when the recipient is entitled to have it. This includes the personal data relating to internal colleagues. Where it is necessary to share personal data with external organisations on a regular basis, data sharing agreements may need to be put in place and the electronic transmission is subject to VTCT data handling rules. People will often attempt to obtain personal data through deception for example, they may pretend to be the data subject to whom the personal data relates, or they may try to take records from hard-copy files. Similarly, human error is often a factor in breaches of security such as sending data to the wrong recipient or losing unsecured devices. Cyber-attacks are becoming increasingly prevalent, and staff must be alert to any unusual activity or potential assaults on VTCT's security defences. Any concerns relating to the use of personal data, whether real or suspected, must be reported to the DPO via the inbox (DPO@vtct.org.uk).

4. Accountability and Governance

VTCT's approach to data protection management is one of sensible risk management and continual improvement which is driven by VTCT's core values as listed below:

- Partnership: be on the side of our customers and learners
- Ease: Simplify complexity to identify the best route forward
- Expertise: Lead with confidence, using our heritage and experience
- Collaboration: Work together for greater impact; don't do it alone
- Energy: Inspire others with passion and warmth

5. Company Responsibilities

As an employer, VTCT recognises its corporate responsibility under the Act as data controller in respect of staff personal data processed for the purposes of administration of employment and management of staff. VTCT is also the data controller in relation to the personal data (business contact details) VTCT records relating to third party suppliers.

In respect of learner data, each party shall be a data controller in respect of any personal data.

The DPO is responsible for data protection compliance and is required to draw up guidance and promote compliance with this policy in such a way as to ensure the easy, appropriate and timely provision of guidance and compliance information.

All new members of staff must receive an introductory briefing on the Data Protection Policy as part of their induction.

6. Staff Responsibilities

All staff, particularly those engaged in accessing or processing of personal information about learners, centre contacts, other staff members or other individuals must comply with the requirements of this policy.

Staff must ensure that:

- All personal information entrusted to them in the course of their employment is kept confidential and stored securely
- No personal information is disclosed either verbally or in writing, accidentally or otherwise to any unauthorised third party
- Where they are unsure about authorised third parties to whom they can legitimately disclose personal/sensitive data they seek advice from their line manager or the DPO

7. Contractor/Casual Staff Responsibilities

VTCT is responsible for the use made of personal data by anyone working on its behalf. Managers who engage contractors or employ casual staff must also comply with this policy and ensure that:

- Any personal data collected or processed during work undertaken for VTCT is kept securely and confidentially. This applies equally to where the data is an integral part of the work, or where it is contained on media etc. which is accessed and applies whether or not VTCT has made specific mention of the data in the contract for work/services
- All personal data is returned to VTCT on completion of the work, including any copies that may have been made. Alternatively, the data is securely destroyed and VTCT receives notification in this regard from the contractor or casual member of staff

- VTCT receives details of any disclosure of personal data to any other organisation, subcontractor or any person who is not a direct staff of the contractor
- Any personal data made available by VTCT or collected in the course of the work is neither stored nor processed outside the European Economic Area (EEA) without formal written consent from VTCT
- All practical and reasonable steps are taken to ensure that contractors, short term or other casual staff do not have access to any personal data beyond what is essential for the work to be carried out properly

8. Responsibilities on termination or change of employment

After termination or change of employment, all staff must continue to:

- Maintain confidentiality of personal information
- Not disclose company confidential information to unauthorised third parties
- Maintain adherence to the UK GDRP and Data Protection Act (2018) regulations This applies to contractors and casual staff, as well as permanent employees.

9. Data Subject Rights

The Data Protection Act provides the following rights for individuals:

- The right to be informed – Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement which is usually satisfied by the provision of a privacy notice (described in further detail below) at the point where the personal data is collected by VTCT
- The right of access – Individuals have a right to access their personal data which is commonly referred to as a Subject Access Request (SAR)
- The right to rectification – Individuals have a right to have inaccurate personal data rectified, or completed if it is incomplete. This right is closely linked to the accuracy principle
- The right to erasure – Individuals have a right to have personal data erased which is also known as the right to be forgotten. This right is not absolute and only applies in certain circumstances
- The right to restrict processing – Individuals have the right to request the restriction or suppression of their personal data. This right is not absolute and only applies in certain circumstances
- The right to data portability – Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This right allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without restriction and without it affecting usability

- The right to object – Individuals have the right to object to the processing of their personal data in certain circumstances, including an absolute right to stop their data being used for direct marketing
- Rights in relation to automated decision making and profiling – Individuals have the right not to be subject to a decision based solely on automated decision-making using their personal data

10. Subject Access Requests

VTCT is required to provide individuals with access their own personal data held by VTCT via a subject access request. Any individual wishing to exercise this right must do so in writing or verbally to the DPO at the address listed in the Contacts section. This does not prevent staff requesting copies of personal data items routinely available from HR should they wish to do so.

All staff receiving a formal request from a data subject wishing to exercise any of the above rights must forward the request immediately to the DPO to arrange fulfilment. Only approved staff who are appropriately trained are permitted to respond to data subject access requests.

VTCT aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within the time limits set down by the Data Protection Act, i.e. 31 days.

More details are available in the document: “GDPR Subject Access Request Process and Right to Erasure Process”.

11. Personal Data Systems

The IT department will maintain an inventory of all electronic systems which include personal data held within VTCT.

12. Register of Processing Activities

The DPO will maintain a register of personal data processing activities in electronic form as part of VTCT’s record keeping responsibilities as a data controller. This register should be disclosed to the Information Commissioner’s Office (ICO) upon request.

13. Data Breach Reporting

Any breach of this Policy, whether real or suspected, or potential breach of the Act, including but not limited to misuse, unauthorised access, potential unauthorised disclosure (including verbal disclosure), loss, damage and destruction of personal data or the VTCT systems and equipment used for processing must be reported in accordance with the Data Breach Policy and the Incident Management Policy and to the DPO (DPO@vtct.org.uk).

All reports of any suspected breach of the Act or the requirements of this Policy will be recorded, investigated and, where proven, may result in disciplinary action, up to and including dismissal or result in referral to law enforcement or regulatory bodies where warranted. Contractors and third parties responsible for non-compliance may have their contracts terminated.

Under no circumstances must staff attempt to prove, 'test' or investigate any perceived security incident unless they are specifically authorised to do so by the DPO.

14. Complaints

For information on VTCT's complaints handling policy, please see the Complaints Policy and Procedures document, available on the VTCT Skills website.

15. Information Security and Data Transmission

VTCT has a legal obligation to protect personal data throughout its lifetime, from creation to destruction, and is aware of its legal obligations under the Act. VTCT's ISMS framework provides robust technical and organisational security controls designed to meet this obligation.

As part of this security framework and to ensure a common approach to data transfers is implemented across the organisation, the Information Classification Policy and Information Handling and Transfer Procedure apply to both personal data and sensitive business and commercial data.

15.1. VTCT Statutory Reporting

VTCT has a statutory obligation to provide data (in an approved and documented format) to its regulators. These reports are produced (normally quarterly) and submitted by various teams via, for example, RITS, SQA portal and email – e.g.:

- Ofqual returns
- Bath Data returns
- TS Series exam returns

15.2. Classification of Data

VTCT classifies information in accordance with the Information Classification Policy and information is handled per the Information Handling and Transfer Procedure. For the avoidance of doubt, any information containing personal data (which could result in an individual being identified) will always have an Internal categorisation as a minimum and consideration should be given as to whether Sensitive is the appropriate categorisation.

16. Contacts

General enquiries regarding VTCT's policy and approach to management and compliance with the Data Protection Act incorporating the EU General Data Protection Regulations may, in the first instance, be addressed to VTCT's Customer Support Team – customersupport@vtct.org.uk or by phone to VTCT's main switchboard – 02380 684500

More specific enquiries, data subject right fulfilment requests and complaints relating to data protection must be addressed to:

Data Protection Officer
VTCT Skills
Aspire House
Annealing Close
Eastleigh
Hampshire
SO50 9PX

17. Compliance, Audit and Review

For details regarding the compliance requirements and compliance breach penalties of this document, the audit criteria, and the review frequency, please see sections 9, 10 and 11 of the Information Security Policy.