Data Protection Policy

March 2021

Version 12.0

Contents

1. Introduction 3
2. Scope 3
   2.1. Personal Data 3
   2.2. Special Category Data 3
3. Policy 4
4. Principles 4
5. Accountability and Governance 6
6. Company Responsibilities 6
7. Staff Responsibilities 6
8. Contractor/Casual Staff Responsibilities 7
9. Data Subject Rights 7
10. Subject Access Requests 8
11. Personal Data Systems 8
12. Register of Processing Activities 8
13. Data Breach Reporting 9
14. Complaints 9
15. Information Security and Data Transmission 10
   15.1. VTCT Statutory Reporting 10
   15.2. Classification of Data 10
16. Contacts 10
17. Related Documents 11
18. Compliance Statement and Consequences of Non-Compliance 11
19. Exceptions 11
20. Audit 11
21. Policy Information Classification 11
22. Review 11

Appendix 1 – Good practice in information handling 12

Appendix 2: Staff Data Protection and Privacy Notice 15

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 (the Act) incorporating the EU General Data Protection Regulation (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 with regard to 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 in accordance with the Act and has chosen to adopt recognised privacy and security standards of best practice (ISO 27001 and BS 10012) 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 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.

3. Policy

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.

4. 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 ICT Department for secure cleansing prior to re-issue or destruction. Personal data must not be retained 'just in case' it might be useful at a later date. 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 7 years 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 organisation Information Asset Register. 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 defenses. Any concerns relating to the use of personal data, whether real or suspected, must be reported to VTCT's Data Protection Officer via the inbox (DPO@vtct.org.uk).

5. 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:

- Together VTCT talk listen and lead: VTCT act with courage and openness to create shared solutions.
- What have VTCT done today to makes us feel proud? VTCT innovate and improve through VTCT's passion for excellence and relationships.
- Trust me to run with it: VTCT have freedom, empowerment and ownership to get a great job done.
- VTCT grow great people: VTCT achieve success by valuing, supporting and investing in colleagues and customers.
- Together VTCT complete the puzzle: VTCT reach out across boundaries to support and collaborate.
- VTCT's Community: VTCT are welcoming, creative and vibrant, achieving great things for VTCT's customers and beneficiaries.

6. 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 ISO 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 Act as part of their induction.

7. 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 VTCT's DPO.

8. 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 the 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

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 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 ICT Department will maintain an inventory of all electronic systems which include personal data held within VTCT.

12. Register of Processing Activities

The ISO will maintain a register of personal data processing activities in electronic form as part of VTCTs 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 **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.

More details are available in the documents:

- Supplier Security Policy
- Incident Management Policy

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

The DPO will co-ordinate appropriate responses to any complaints received in respect of this policy. The complaint must be addressed to the DPO in the first instance. Complaints must be acknowledged immediately and every reasonable effort made to provide a comprehensive reply within 21 days.

If the complainant is not satisfied with the reply then they must inform the DPO within 21 days and will be dealt with in accordance with VTCT's General Complaints Procedure or the VTCT Grievance Procedure as appropriate.

If complainants are dissatisfied with the outcome of the Complaints Procedure relating to personal data processing they are entitled to seek an independent assessment from the ICO. Requests for review by the ICO must be made in writing to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 01625 545700

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 categorization as a minimum and consideration should be given as to whether Sensitive is the appropriate categorization.

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
Aspire House
Annealing Close
Eastleigh
Hampshire
SO50 9PX

17. Related Documents

This document must be read in conjunction with VTCT **Information Security Policy**.

18. Compliance Statement and Consequences of Non-Compliance

All staff, contractors and suppliers will need to comply with the requirements of this policy and all are expected to be familiar with the contents therein. Any breaches of VTCT information security or data protection policies will be logged and may be subject to a formal security investigation.

Where proven, failure to comply will result in disciplinary action being taken against individuals determined to be responsible for the breach under VTCT disciplinary procedures up to and including summary dismissal for gross misconduct. VTCT may also initiate legal action or refer the breach to relevant law enforcement and regulatory authorities where warranted. Non-compliance by contracted third parties or their employees may result in termination of the supplier's contract.

19. Exceptions

Where a VTCT information security policy, data protection policy, or technical standard's requirement cannot be met for any reason, a formal request for exception must be submitted in writing to the ISO for approval. Failure to obtain exception approval will be considered a breach of this policy.

20. Audit

Audit spot checks and automated monitoring may be conducted to ensure compliance with this Policy. Any non-compliance identified during an audit must be reported to the DPO in the first instance to initiate investigation of any associated incident.

21. Policy Information Classification

VTCT information security policies are classified as 'internal use only'. Unless otherwise stated, no part or extract from them or the associated files held on VTCT's computer networks, systems or devices may be distributed to any external organisation without the express permission of the DPO or ISO.

22. Review

This Policy will be reviewed on an annual basis, unless changes to business operations, relevant legislation, regulations, contractual commitments or codes of practice necessitate an earlier amendment.

Appendix 1 – Good practice in information handling

Who is this guide for?

This guide has been written for all VTCT staff who collect, manage, transfer or use data about learners, staff or other individuals during the course of their work. Its aim is to raise awareness of where potential breaches of security could occur.

Following these guidelines will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation VTCT might suffer if you lose personal data about individuals.

Your roles and responsibilities

As a staff or contractor of VTCT, you have a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

Why protect information?

VTCT holds personal data on learners, staff and other people in the course of its daily business activities. Some of this data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data could result in adverse media coverage, and potentially damage the reputation of VTCT. This can make it more difficult for VTCT to use technology to benefit learners.

What Information do you need to protect?

You must secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to VTCT – see section 15.2 of this document. As with any organisation, VTCT has a Data Protection Officer. This falls within the remit of the Chief Academic Officer (CAO), who has responsibility for working out exactly what information needs to be secured, how information is securely handled, how the information changes over time, who else is able to use it and why.

Data security do's and don'ts

There are plenty of things that you must do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these guidelines will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

When working online:

Do…

- Make sure that you follow VTCT's policies on keeping your PC(s) up to date with the latest security updates and make sure that you keep any computers that you own up to date. Get advice from the ICT Department if you need help

- Turn on relevant security warnings in your web browser (for example, the automatic phishing[1] filter available in Internet Explorer)
- Make sure that you only install software that the ICT team has checked and approved and only download files or programs from sources you trust. If in doubt, talk to the ICT Department
- Ensure that you have read and understood the acceptable-use policies which are available on the Organisational Docs/Tech Division tab on the Intranet and ensure you follow them

Don't…

- Browse sites that are not business-related or are prohibited under the Acceptable Use of Assets policy. Remember VTCT reserves the right to monitor websites which staff are visiting
- Enter credit card or payments details into any site that does not have a valid security certificate, and where the URL does not start with "https://"

Email and messaging:

Do…

- Read the VTCT relevant policies available on the Intranet and report any spam or phishing emails to the ICT Department that are not blocked or filtered
- Report phishing emails to the organisation they are supposedly from
- Use the VTCT contact/address books contained within Outlook. This helps to stop email being sent to the wrong address
- Encrypt[2] any attachments to emails which contain personal information and do not include personal information in the body of the email

Don't…

- Click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on
- Turn off any email security measures that the ICT Department has put in place or recommended
- Email sensitive information unless you know it is encrypted. Talk to the ICT Department for advice
- Try to bypass VTCT's security measures to access your email off-site (for example, forwarding email to a personal account)
- Reply to chain emails

Passwords:

Do…

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- Make your password easy to remember, but hard to guess

[1] Phishing is an attempt to obtain your personal information (for example, account details) by sending you an email that appears to be from a trusted source (for example, your bank).

[2] Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it.

- Change your password(s) if you think someone may have found out what they are, in any event, change them at least every three months

Don't…

- Share your passwords with anyone else
- Write your passwords down
- Use your work passwords for your own personal online accounts
- Save passwords in web browsers if offered to do so

Appendix 2: Staff Data Protection and Privacy Notice

VTCT takes great care to protect the personal information of all data subjects with whom the company interacts.

Data Controller

As your employer, VTCT assumes the responsibilities required of a data controller under the UK Data Protection Act 2018 (incorporating the EU General Data Protection Regulation 2016). A key responsibility is to inform you about how and why VTCT processes your personal data. This notice is designed to fulfil that obligation.

When you become staff or contractor VTCT collects and processes your personal data where this is necessary for the purposes of administration of your employment, benefits administration, remuneration and for managing VTCT's employees. Your contract of employment or contractor agreement provides the legitimate basis for this processing.

VTCT Data Protection Policy

VTCT has established this policy to provide protection for the rights and freedoms of data subjects over the processing of personal data that is applicable to all staff (whether temporary, including associate contractors, or permanent). This document includes guidelines on how to comply and the latest version is published on the intranet.

Categories of Data Processed

In the context of employment, VTCT processes the following categories of personal information where necessary, and where VTCT is required to do so by law:

- Name and contact information (address details, telephone numbers, email address)
- Place of birth, gender, nationality and passport (or equivalent national identity papers)
- Photographs and CCTV images
- Evidence of marital status, family, spouse and dependent's details and next of kin
- Recruitment data (e.g. CVs), including languages, references, qualifications, employment and education history
- Training and skills development information
- Membership of professional societies and internal teams
- Employment vetting, including right to work checks
- Employment contract or contractor agreement, roles and job placement, including project assignment and management reporting
- Staff management data including onboarding, role changes, performance, service history, annual leave, special leave such as maternity, paternity leave, teleworking details, travel details, resignation, grievance and disciplinary information.
- National driving licences and vehicle registration
- Financial information including salary and payroll data, pensions, travel and other expenses, bank account details or tax forms
- Physical and mental health information including sick leave, fit notes, medical history and medical reports where applicable.

- Ethnicity/equal opportunities monitoring

Recipients of the Data Processed

Where necessary for the purposes detailed above, and only in limited circumstances, such as when VTCT are required to do so by law, VTCT may share (or grant access to) your personal data with external official authorised bodies and regulators including:

- DVLA
- Department of Work and Pensions
- Financial accountants
- Screening & vetting partners
- Workplace pension scheme administrators
- HMRC and other government and regulatory bodies
- Service providers or other partners who help us manage VTCT's business who may, provide travel services, perform statistical analysis, host and manage or support VTCT's IT systems and software, or provide services to manage access to VTCT offices.

Where this is necessary, data sharing agreements ensure that your rights are maintained by VTCT's partner organisations.

VTCT may share your personal data with training course providers and event organisers.

VTCT only permit the transfer of your personal data outside of the EEA or to another international organisation if it is determined that adequate safeguards are in place to protect your rights over the processing of your personal data.

Special Category Personal Data

VTCT will only process staff special category data (e.g. physical and mental health or disability, ethnic origin, religious, political or other beliefs, trade union membership, genetic or biometric data, sexual orientation including transgender and criminal convictions/alleged offences) where this is necessary in relation to your employment or where VTCT are required to do so by a law or a regulatory obligation or where this is necessary in the context of your employment contract.

VTCT do not require your consent for this as an exemption applies. However, if VTCT use your personal information for any other reason VTCT will require your explicit consent to do so.

Staff Vetting and Screening

VTCT may use your personal information to undertake staff screening and vetting where VTCT are required to do so, e.g. to satisfy government requirements to check eligibility to work in the UK or where a specific role requires us to screen staff for trustworthiness and reliability as mandated by a regulator.

Vetting may include an enhanced disclosure of criminal convictions or alleged criminal offences and special measures are required to justify this type of vetting and ensure that any such disclosure is conducted directly between staff and the vetting authority. VTCT will not collect or record criminal conviction information internally, only the outcome.

Credit checks may also be performed where employees are deployed in a role that carries a financial position of trust.

Data Retention

VTCT will retain your personal data in an identifiable form only for as long as is necessary and in accordance with the VTCT's Data Retention Policy (draft).

Non-essential HR records will be removed from HR files after a period of 12 months from staff leaving date. Essential HR records including salary, tax, payroll and benefits information will be retained for a period of 6 years following termination of your employment. Associated financial records will be retained for 6 years following financial audit. This is necessary as VTCT is required to keep specific records to comply with legal obligations.

The following data records are also retained for a specific amount of time:

- Annual leave, sick leave, and special leave records will be retained for 3 years.
- Parental leave records will be retained for 5 years from the birth of a child /adoption date.
- Pension information will be retained for 12 years after the benefit ceases.
- CCTV images will be retained for a maximum of 1 year.
- Entries reported in Accident Books for health and safety purposes will be retained indefinitely.

Security of your Personal Data

VTCT adopts recognised security best practice standards and techniques to protect your personal data from unauthorised access, use or disclosure. VTCT have adopted formal processes to deal with any suspected security incidents that may include notifying you of any breaches of your personal data or formal notification to the UK/EU Data Protection supervisory authorities.

Right of Access, Rectification, Erasure and Portability

As defined earlier in this policy, staff have a right to access a copy of their personal data as well as to have any inaccurate data corrected and, in limited circumstances, erased or passed to another data controller in electronic format. If you are a current staff or contractor, you can do this by contacting the Head of HR who will action your request where this falls within HR current working practice. If HR are unable to provide the personal data requested as part of routine service, or if you are a former staff or have any difficulties, you must contact the DPO, in writing via DPO@vtct.org.uk who will advise you what to do.

Please ensure that you inform HR of any changes to your personal data to ensure VTCT can keep your staff information up-to-date. You must also report any incidents involving misuse or unauthorised disclosure of personal data to DPO@vtct.org.uk or to the DPO or ISO in confidence.

If you have a concern or complaint about the way that your personal data has been, or is being processed, please direct it to the DPO and VTCT will try to resolve any issues initially. If VTCT are unable to do that for any reason, you also have a right to lodge a complaint with the UK Information Commissioner (ICO) and further information on your rights and how to exercise them is available on www.ico.org.uk.

Changes to this Data Protection Policy

VTCT will occasionally update this Data Protection Policy to reflect organisational changes and feedback. VTCT encourage you to periodically review this policy to stay informed on how VTCT use and protect your data.

Document amendment history page

Version	Document Owner	Issue Date	Changes	Role
10.0	Head of ICT	02/10/2019	Alignment with ISO 27001	Head of ICT
10.1	Head of ICT	06/10/2020	Updates due to organization changes	Head of ICT
11.0	Head of ICT	09/11/2020	Signed-Off	Head of ICT
12.0	Chief Academic Officer	18/03/21	Signed-Off	Data Protection Officer

Document Review

Role	Review Status
ICT Manager	Review complete
Chief Academic Officer	Review and minor edit complete

Document Owner

Document Owner	Document shared with
Chief Academic Officer and Data Protection Officer	Head of ICT and Information Security Officer

Document Sign-off

Role	Sign-off Date
CAO and DPO	18/03/21