Data Protection Policy

March 2018

Version 5

Contents

1. Introduction 3
2. Scope 3
3. Company Responsibilities 4
4. Staff Responsibilities 4
5. Contractor/Casual Staff Responsibilities 4
6. Subject Access Requests 5
7. Personal Data Systems 5
8. Charges 5
9. Data Security Breach 5
10. Complaints 5
11. Data Encryption 6
    11.1. Our Responsibilities 6
    11.2. Types of Data 6
        11.2.1. Learner Data 6
        11.2.2. Commercial Data 6
12. Contacts 7
13. Related Documents 7
14. Appendix 1: Good practice in information handling 8
    14.1. Data security do's and don'ts 8
    14.2. Your roles and responsibilities 8
    14.3. Why protect information? 8
    14.4. What information do you need to protect? 8
    14.5. Steps you can take to help prevent security problems 8
        14.5.1. When working online 8
        14.5.2. Email and messaging 8
        14.5.3. Passwords 9
        14.5.4. Laptops/PCs 10
        14.5.5. Sending and sharing data 10
        14.5.6. VTCT or sent by post/courier. 10
        14.5.7. When working off-site 10

1. Introduction

VTCT takes its responsibilities with regard to the management of the requirements of the Data Protection Act 1998, and subsequent amendments, very seriously. This document provides the policy framework through which this effective management can be achieved and audited.

VTCT recognise that in order to carry out our services, we must collect personal data relating to the usage of our systems by our clients and their users.

“Personal data” means any information relating to a living individual from which that individual may be identified (including, for example, their name or address).

VTCT will manage any personal data in accordance with the Data Protection Act 1998 and other related legislation, in whichever manner that such data is collected, recorded or used (whether on paper, databases, emails, CCTV or telephone records, or recorded by any other means).

2. Scope

The purpose of this policy is to ensure that VTCT and its staff comply with the provisions of the Data Protection Act 1998 when processing personal and sensitive data. Any infringement of the Act will be treated seriously by VTCT and may be considered under disciplinary procedures.

VTCT follow the eight data protection principles set out in the Data Protection Act 1998 and understands its obligations to ensure that personal data is managed fairly, lawfully, accurately and securely. These principles require that personal data shall:

- be processed fairly and lawfully;
- be processed for limited purposes;
- be adequate, relevant and not excessive;
- be accurate and up-to-date;
- not be kept for longer than is necessary;
- be processed in line with the rights of data subjects;
- be processed securely;
- not be transferred to a country or territory outside the European Economic Area without adequate safeguards.

Our approach to data protection is one of sensible risk management which is driven by our core values as listed below:

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

3. Company Responsibilities

VTCT recognises its corporate responsibility under the Act and is the data controller. The Data Protection Officer 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 retrieval of information.

The Data Protection Officer has access to all relevant documents relating to a legal compliance request and in conjunction with the CTO and appropriate members of the Management team, will make decisions regarding what information is released or exempted.

All new members of staff should receive an introductory briefing on the Data Protection Act as part of their induction. (See Appendix I)

4. Staff Responsibilities

All staff, particularly those engaged in the access 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 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 Data Protection Officer.

Any deliberate infringement of the Act will be treated seriously by VTCT and may be considered under disciplinary proceedings.

5. 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 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 that 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 or any person who is not a direct employee 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 UK 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.

6. Subject Access Requests

VTCT is required to permit individuals to access their own personal data held by VTCT via a Subject Access Request. Any individual wishing to exercise this right should do so in writing to the Data Protection Officer and a charge may be made for this request.

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.

Individuals will not be entitled to access information to which any of the exemptions in the Act applies. However, only those specific pieces of information to which the exemption applies will be withheld, and information covered by an exemption will be subject to review by the Data Protection Officer.

7. Personal Data Systems

The ICT Department will maintain a register of all electronic systems which include personal and sensitive data held within VTCT.

8. Charges

VTCT currently charges £10 to make a subject access request, however, VTCT reserves the right to review this fee at any time.

9. Data Security Breach

Any breach of the Data Protection Act and the requirements of this Policy should be reported to the Data Protection Officer as soon as possible.

A report of a suspected breach of the Act will be dealt with in accordance with the VTCT complaints procedure.

10. Complaints

The Data Protection Officer will co-ordinate any complaints received in respect of this policy. The complaint should be addressed to the Data Protection Officer in the first instance. Complaints will be acknowledged immediately and every reasonable effort will be made to offer a comprehensive reply within 21 days.

If the applicant is not satisfied with the reply then they should inform the Data Protection Officer within 21 days. The complaint will then be forwarded to the Director of Operations and will be dealt with in accordance with VTCT's General Complaints Procedure or the VTCT Grievance Procedure as appropriate.

If applicants are dissatisfied with the outcome of the Complaints Procedure they may seek an independent review from the Information Commissioner. Requests for review by the Information Commissioner should be made in writing to:

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

11. Data Encryption

VTCT has a legal obligation to protect personal information and is aware of its legal obligations under the Data Protection Act 1998. For more information, visit the website of the Information Commissioner's Office (http://www.ico.gov.uk).

To comply with our current DPA registration and ensure a common approach to data transfer across the organisation, the following procedure should be adopted to cover the transmission of ALL data from VTCT to Centres and other Stakeholders.

11.1. Our Responsibilities

We have a statutory obligation to provide data (in an approved and documented format) to our 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

11.2. Types of Data

Our data falls into 2 main types:

- Learner sensitive data
- Commercially sensitive data

11.2.1. Learner Data

VTCT No.	Forename	Surname	ULN	SCN	DOB	Address	Postcode

In the example above – should a data request include one or more of the items highlighted, the data is "sensitive" and needs to be transmitted in a secure way. It must not be sent via email without encryption.

11.2.2. Commercial Data

VTCT Centre No.	Centre Name	NCN	Address	Turnover	No. of Learners	+/- turnover from last year

In this example – the provision of attributable financial information would be considered as commercially sensitive data and if one or more of the examples highlighted are included, some encryption of the file transfer should be in place.

VTCT Centre No.	Centre Name	Address	Main Contact	Sector	VTCT League Position	No. of Learners

In this example, provision of the highlighted data provided could allow a competitor to target a specific market sector – as such it would be regarded as commercially sensitive.

The tables above are only "examples" of where data should be treated as sensitive and are not exhaustive.

12. Contacts

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

More specific enquiries, data requests and complaints should be addressed to:

Pete Kelly
Chief Technical Officer
VTCT
Aspire House,
Annealing Close,
Eastleigh,
Hampshire,
SO50 9PX

13. Related Documents

This document should be read in conjunction with VTCT ICT Policy.

14. Appendix 1: Good practice in information handling

14.1. Data security do's and don'ts

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.

14.2. Your roles and responsibilities

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

14.3. 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.

14.4. What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to VTCT – see page 4 of this document. As with any organisation, VTCT has a Data Protection Officer. This falls within the remit of the ICT Manager, 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.

14.5. Steps you can take to help prevent security problems

There are plenty of things that you should 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.

14.5.1. 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 team if you need help;
- only visit websites that are allowed by VTCT. Remember VTCT reserves the right to monitor websites which staff are visiting;
- turn on relevant security warnings in your web browser (for example, the automatic phishing 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 team;
- ensure that you have read and understood the acceptable-use policies which are available on the ICT tab on the Intranet and ensure you follow them.

14.5.2. Email and messaging

Do:

- read the VTCT email policy available on the Intranet under the ICT tab and report any spam or phishing[1] emails to the ICT team 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.

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 team has put in place or recommended;
- email sensitive information unless you know it is encrypted[2]. Talk to the ICT team 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.

14.5.3. 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;
- 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.

[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.

14.5.4. Laptops/PCs

Do

- shut down your PC/Laptop using the 'Shut Down' or 'Turn Off' option;
- try to prevent people from watching you enter passwords or view sensitive information;
- turn off and store your laptop securely (if travelling, use your hotel's safe);
- lock your desktop/laptop when leaving it unattended;
- make sure your PC/Laptop is protected with encryption software.

Don't

- use public wireless hotspots – they are not secure;
- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot;
- let unauthorised people use your laptop;
- use hibernate or standby.

14.5.5. Sending and sharing data

Do

- be aware of who you are allowed to share information with. Check with the ICT Manager if not sure;
- ask third parties how they will protect sensitive information once it has been passed to them;
- encrypt all removable media (e.g. USB sticks, CDs, portable drives) taken outside of.

14.5.6. VTCT or sent by post/courier.

Do

- lock sensitive information away when left unattended.

Don't

- send sensitive information (even if encrypted) on removable media if secure remote access is available;
- send sensitive information by email unless it is encrypted;
- assume that third-party organisations know how your information should be protected.

14.5.7. When working off-site

Do

- wherever possible access data remotely instead of taking it off-site;
- make sure you sign out completely from any services you have used;
- try to reduce the risk of people looking at what you are working with;
- check with the ICT Dept. if you are taking your laptop abroad on business as some countries restrict or prohibit encryption technologies.

Don't

- take information off-site that you are not authorised to;
- leave your laptop, portable devices etc. unattended;
- attempt to access the VTCT network on equipment not owned/virus checked by VTCT.

Document History

Version	Issue Date	Changes	Role
v1	12/10/2019	First Published	IT Manager
v1.1	15/10/2010	Review after BSI CPA Conference/workshop – addition of exclusions and ongoing monitoring	IT Manager
v1.2	15/10/2011	Annual Review	IT Manager
v1.3	07/11/2012	Annual Review	IT Manager
v1.4	07/02/2013	Amendment of contact details	IT Manager
v1.5	10/12/2013	Annual Review	IT Manager
v2	15/07/2015	Policy Review	Customer Support Manager
v2.1	01/06/2016	Update to include data encryption guidance	Customer Support Manager
v3.0	24/02/2017	Amalgamation of policies technical review	Chief Technical Officer
v3.1	27/02/2017	Formatting amendments	Qualifications Officer
v3.2	12/04/2017	Updated Branding	Quality and Processing Supervisor (Eastleigh)
v4	12/02/2018	Formatted and amended to new branding	Product Administrator
v4.1	15/03/2018	Missing Highlighting added to tables in 11.2	Strategy and Projects Manager
V5	15/03/2018	V4.1 changes signed off as final	Chief Technical Officer

Document Review

Role	Review Status
Director of Operations	Reviewed
Customer Support Manager	Reviewed
Chief Technical Officer	Reviewed

Document Sign-off

Role	Sign-off Date
Chief Technical Officer	15/03/2018