

General Data Protection Policy

Document Owner	Compliance Officer / Managing Director
Date Approved	November 2025
Approved by	Managing Director
Last Review	May 2024
Next Review	November 2027

Version Control

Revision #	Date	Revision summary	Reviewed by
1	27 Sept 2021	Updated	KA HRV
2	31 st August 2022	Updated DP Officer to Geoffrey Arthur	MC
3	November 2023	Update DP Officer to Helen Lloyd-Hole.	CG
4	May 2024	Update DP Officer to CM	CM

5	November 2025	Updated owner of document to include Managing Director	CM
---	---------------	--	----

Contents

1.	Introduction.....	3
2.	Purpose	3
3.	Scope.....	4
4.	Legislation.....	4
5.	Definitions	4
6.	Data protection principles	4
7.	Individual rights	5
8.	Subject Access Requests.....	5
9.	Other rights.....	6
10.	Data security	6
11.	Impact Assessment	7
12.	Data Breaches	7
13.	Individual Responsibilities.....	7
14.	Training.....	8
15.	The General Data Protection Regulation (GDPR)	8
16.	The General Data Protection Regulation (GDPR)	8
	Policies, Procedures & Forms.....	8
17.	Review	9
18.	Quality Assurance	9

1. Introduction

This policy sets out WBTC's approach to data protection and reflects the requirements of the General Data Protection Regulation (GDPR), which will come into effect in the UK on 25 May 2018. The Data Protection Bill, which will repeal and replace the Data Protection Act 1998, is currently being considered by UK Parliament (April 2018). The Data Protection Bill supplements the GDPR and contains additional requirements regarding special categories of personal data, data on criminal convictions and offences, information requirements for individuals and subject access requests.

2. Purpose

WBTC is committed to being transparent about how it collects and uses the personal data of its workforce and to meeting its data protection obligations. This policy sets out WBTC's commitment to data protection and individual rights and obligations in relation to personal data.

WBTC has appointed Craig Mincher (Managing Director) as the person with responsibility for data protection compliance within WBTC. They can be contacted at Craig@wbtc-uk.com. Questions about this policy or requests for further information, should be directed to them.

3. Scope

This policy applies to the personal data of learners, subcontractors, suppliers, job applicants, Staff (workers, contractors, volunteers, interns, apprentices) and former Staff.

4. Legislation

The policy reflects national legislation and guidelines on good practice:

- Data Protection Act 2018 (DPA 2018)
- UK General Data Protection Regulation (UK GDPR)

WBTC is committed to implementing all current data protection legislation. We keep legislation under review to ensure our full compliance.

5. Definitions

"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.

"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.

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

6. Data protection principles

WBTC processes HR-related personal data in accordance with the following data protection principles:

- WBTC processes personal data lawfully, fairly and in a transparent manner.
- WBTC collects personal data only for specified, explicit and legitimate purposes.
- WBTC processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing or requirements as set out by the Education and Funding Skills Agency (EFSA).
- WBTC keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- WBTC keeps personal data only for the period necessary for processing.
- WBTC adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- WBTC keeps learner data for a period as prescribed by the relevant legislation.

WBTC publishes 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.

Where WBTC processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with legislation.

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

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personal file (in hard copy or electronic format or both) and on electronic systems. The periods for which WBTC holds personal data are contained in its privacy notices to individuals and the reasons why we hold data and how long data is held for.

WBTC keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR) for example the Equality & Diversity monitoring form is held to ensure there is no bias and to comply with the Equality Act 2010.

7. Individual rights

As a data subject, individuals have a number of rights in relation to their personal data under the GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

8. Subject Access Requests

Individuals have the right to make a subject access request. Please also refer to coded document **H16 Subject Access Request Procedure GDPR**. If an individual makes a subject access request, WBTC will tell them:

- whether or not their 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;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if he/she thinks WBTC has failed to comply with his/her data protection rights; and
- whether or not WBTC carries out automated decision-making and the logic involved in any such decision-making.

WBTC 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.

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

To make a subject access request, the individual should send the completed request form (coded document **H12 Subject Access Request Form**) to Craig@wbtc-uk.com. In some cases, WBTC may need to ask for proof of identification before the request can be processed. WBTC will inform the individual if it needs to verify his/her identity and the documents it requires.

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

If a subject access request is manifestly unfounded or excessive, WBTC is not obliged to comply with it. Alternatively, WBTC 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 WBTC has already responded. If an individual submits a request that is unfounded or excessive, WBTC will notify them that this is the case and whether or not it will respond to it.

9. Other rights

Individuals have a number of other rights in relation to their personal data. They can require WBTC to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override WBTC's legitimate grounds for processing data (where WBTC relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override WBTC's legitimate grounds for processing data.

To ask WBTC to take any of these steps, the individual should send the request to Craig@wbtc-uk.com.

10. Data security

WBTC takes the security of personal data seriously. WBTC 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 Staff in the proper performance of their duties.

Where WBTC engages third parties to process personal data on its behalf ("data processors"), such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

11. Impact Assessment

Some of the processing that WBTC carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, WBTC 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. Instances that are likely to qualify as high risk to the rights and freedoms of individuals include where an employer conducts systematic monitoring of Staff or processes special categories of personal data or data on criminal convictions and offences.

12. Data Breaches

If WBTC discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Any data breach should be reported here: <https://ico.org.uk/for-organisations/report-a-breach/>). WBTC will record all data breaches regardless of their effect on the WBTC Personal Data Security Breach log.

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.

13. Individual Responsibilities

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

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, WBTC relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside WBTC) who have appropriate authorisation;
- 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);

- not to remove personal data, or devices containing or that can be used to access personal data, from WBTC's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under WBTC'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.

14. Training

WBTC 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.

15. The General Data Protection Regulation (GDPR)

GDPR requires employers to:

- process personal data lawfully, fairly and in a transparent manner;
- collect data for specified and legitimate purposes and not process data in a manner that is incompatible with those purposes;
- collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- ensure that data is accurate and kept up to date, and take every reasonable step to rectify or erase data that is inaccurate without delay;
- keep data only for the period necessary for the purposes of processing;
- ensure that appropriate security is in place to protect data against unauthorised or unlawful processing, accidental loss, destruction or damage;
- process data in accordance with the rights of data subjects; and
- transfer data outside the European Economic Area (EEA) only if there is an adequate level of protection for the rights and freedoms of data subjects.

16. The General Data Protection Regulation (GDPR)

For more detail of internal policies, security and controls please refer to the following WBTC documents:

Policies, Procedures & Forms

- WBTC Personal Data Breach Procedure GDPR (coded document W153)
- WBTC Personal Data Breach Form GDPR (coded document W154)
- WBTC Personal Data Breach Log (coded document W155)
- Information, Communication and Technology Policy

- ICT Policy & Procedure
- Legal & Privacy Notices
- Employee E-Safety
- Information, Communication and Technology Policy

17. Review

Notwithstanding our current policies and procedures, the Senior Leadership Team reserve the right to amend, curtail or terminate this policy at any time and without notice.

18. Quality Assurance

This Policy will be reviewed every two years, sooner if legislation, best practice or other circumstances indicate this is necessary. It shall remain in force until any alterations are formally agreed.