UK-GDPR (General Data Protection Regulations) Policy

1. Introduction

Ventol Ltd ("the Company") is committed to protecting the privacy, security, and rights of all individuals whose personal data we process.

This policy explains how we handle personal data in line with:

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

This policy applies to all employees, workers, job applicants, former employees, apprentices, placement students, volunteers, contractors, and consultants ("relevant individuals").

All employees handling personal data must follow this policy.

2. Key Definitions

- **Personal Data**: Information that can identify a living person (directly or indirectly), such as name, contact details, ID numbers, location data, online identifiers.
- **Special Category Data**: Sensitive data (e.g., health, race, religion, biometric data).
- **Criminal Offence Data**: Information relating to criminal convictions or allegations.
- **Processing**: Any activity involving personal data—collecting, storing, using, sharing, deleting.
- **Controller**: The organisation deciding how and why personal data is processed.
- **Processor**: A third party that processes data on our behalf.

The Company is the Data Controller.

3. Data Protection Principles

Under UK-GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

1) processing will be fair, lawful and transparent
2) data be collected for specific, explicit, and legitimate purposes
3) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
4) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
5) data is not kept for longer than is necessary for its given purpose
6) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.
7) we will comply with the relevant UK-GDPR procedures for international transferring of personal data

4. What Personal Data We Collect

We collect and process data necessary for managing employment and business operations. This may include:

4.1 Standard Personal Data

- Name, address, phone numbers, email
- Recruitment information (CVs, references, qualifications)
- Pay, tax, National Insurance, bank details
- Job title, terms & conditions, appraisal and performance records
- Training records
- Attendance and annual leave data

4.2 Special Category Data

Processed only when strictly necessary:

- Health and medical information
- Diversity monitoring (race, ethnicity, religion, etc.)
- Trade union membership

4.3 Criminal Records Data

- Disclosure and Barring Service (DBS) information where legally required

5. Why We Process Personal Data (Lawful Bases)

We process personal data only when a lawful basis applies.

5.1 Standard Personal Data

- **Contract (Art 6(1)(b))** – to recruit, employ, pay, and manage individuals
- **Legal obligation (Art 6(1)(c))** – e.g., tax, payroll, employment law, H&S
- **Legitimate interests (Art 6(1)(f))** – e.g., security, business operations

5.2 Special Category Data

Processed under:

- **Employment law obligations (Art 9(2)(b))**
- **Health & safety requirements**
- **Explicit consent (Art 9(2)(a))** – *only where no other basis applies*

5.3 Criminal Offence Data

Processed under:

- **Employment law obligations**
- **Safeguarding and security requirements**

We do **not** rely on consent unless absolutely necessary.

6. How Long We Keep Data (Retention)

Personal data is kept only as long as needed for legal or operational purposes. Key examples:

- Personnel files: 6 years after employment ends
- Payroll/tax information: 6 years
- Training records: 3 years
- Health and safety records: 40 years (where required)

Full details are in the Record Retention Schedule.

7. Your Data Protection Rights

All relevant individuals have the following rights:

1) To be informed
2) To access their data
3) To correct inaccurate data
4) To request erasure
5) To restrict processing
6) To object to processing
7) To data portability
8) To object to automated decision-making or profiling

How to exercise your rights

Email: **dpo@ventol.co.uk**

Requests can be made verbally or in writing.

We respond within **one month** unless legally permitted to extend.

8. Data Access: (Subject Access Requests (SARs)

Employees may request a copy of their personal data.

- No fee unless the request is excessive or repetitive.
- Identity may need to be verified.
- Guidance is available in the SAR Policy.

9. Data Sharing and Disclosures

Data is shared only when necessary and lawful.

Examples include:

- Payroll providers
- Pension and insurance providers
- Occupational health services
- IT and software providers
- Government bodies (HMRC, HSE, Police)
- Legal advisers

All third parties must comply with UK GDPR.

10. Data Security

We protect data using appropriate technical and organisational measures:

- Locked storage for paper records
- Password-protected and encrypted digital systems
- MFA where applicable
- Access restricted on a "need-to-know" basis
- Clear-screen and clear-desk practices

Personal data must not be stored on USB drives, laptops, or personal devices without prior authorisation and encryption.

Failure to follow security rules may result in disciplinary action.

11. Third Party Processors

Any third party processing data for us must sign a Data Processing Agreement and meet our compliance standards.

Vendors are reviewed periodically.

12. International Transfers

The Company does not transfer personal data outside the United Kingdom.

If this changes, employees will be informed of:

- the destination country,
- the transfer mechanism (e.g., IDTA),
- and the safeguards in place.

13. Data Breaches

All data breaches must be reported immediately to the DPO.

The Company will:

- Record all breaches
- Investigate promptly
- Report to the ICO within 72 hours if required
- Notify affected individuals when necessary

See the Breach Notification Policy for details.

14. Training

- All new employees receive data protection training during induction.
- Annual refresher training is mandatory.
- Role-specific training is provided for high-risk roles.

15. Records of Processing

We maintain a Record of Processing Activities (ROPA) documenting:

- what we process
- why we process it
- retention periods
- lawful bases
- data sharing partners

This is reviewed regularly.

16. Data Protection Contact Details

Data Protection Officer (DPO):

Mrs Victoria Franks
Email: **dpo@ventol.co.uk**

Ventol Ltd
Unit 1 & 2, Landsberg
Lichfield Road Industrial Estate
Tamworth, Staffordshire
B79 7XB

17. Approval

Signed:

Mr Luke Corbett
Managing Director

Date: 26 February 2026
Next review: 26 February 2027