Data Protection Policy for Employees, Workers & Consultants

1 Overview and Scope

1.1. This policy outlines how Eat That Frog CIC ('the Company') collects, uses, and safeguards the personal data of employees, workers, volunteers, apprentices, consultants, and contractors in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and ISO 27001 information security standards.

1.2. The Company is committed to protecting the privacy and security of your personal data and will ensure that data is processed lawfully, fairly, and transparently.

1.3. This policy is issued alongside the Employee Privacy Notice, your employment contract, and relevant policies such as our Data Retention Policy, ISMS Policy (under ISO 27001 implementation), and the Cyber Essentials framework.

1.4. The Company's Data Protection Lead is the first point of contact for queries relating to this policy and data rights.

1.5. Eat That Frog CIC is registered with the Information Commissioner's Office (ICO) as a data controller.

1.6. Personal data must be managed in accordance with the organisation's Information Security Management System (ISMS), ensuring appropriate classification, protection, and lifecycle management.

2 Data Protection Principles

In line with the UK GDPR, personal data must:

- Be processed lawfully, fairly, and transparently.
- Be collected for specified, explicit, and legitimate purposes.
- Be adequate, relevant, and limited to what is necessary.
- Be accurate and kept up to date.
- Not be kept for longer than necessary.
- Be processed securely.

3 Definitions and Data Covered

3.1. **Personal Data**: Any information relating to an identifiable individual, directly or indirectly (e.g. name, ID number, IP address, etc.).

3.2. **Special Category Data**: Sensitive data such as health information, ethnicity, religious beliefs, or biometric data.

3.3. Examples of data we may collect include:

- Employment records, pay and benefits, performance records.
- Health and disability data.
- Emergency contacts.
- Right-to-work documents and background checks.
- CCTV and access logs.
- Training records.
- Communications on company systems.

3.4 Data Classification

All personal data must be classified in line with the Data Security Policy as:
· Internal
· Confidential
· Highly Confidential

The classification determines the level of protection, access control, and handling requirements applied to the data.

4 How Data Is Collected

Data is collected:

- During recruitment and onboarding.
- Through employment relationship (e.g. performance reviews, training, absence records).
- Via third parties (e.g. DBS, previous employers);
- Automatically (e.g. email metadata, building entry systems).

The Company may monitor the use of its systems, including email, internet usage, and access logs, to ensure security, compliance, and operational effectiveness. Monitoring will be proportionate, lawful, and communicated transparently.

5 Lawful Basis for Processing

We will only process your data where legally permitted, including:

- To fulfil employment contracts.
- To comply with legal obligations (e.g. safeguarding, tax reporting);
- Where there is a legitimate interest (e.g. business continuity, performance monitoring);
- Where consent is given (e.g. promotional photos);
- To protect vital interests.

6 Data Security and Retention

6.1 All personal data must be protected using appropriate technical and organisational measures, including:
· Role-Based Access Control (RBAC) to restrict access to authorised users only
· Multi-Factor Authentication (MFA) where appropriate
· Secure storage on centrally managed systems
· Encryption of sensitive data in transit and at rest
· Regular system patching and malware protection

6.2 Systems must maintain appropriate audit logs of access and activity relating to personal data.

6.3 Personal data must not be stored on personal or unauthorised devices.

6.4 Data retention and disposal must be carried out in accordance with the Data Retention Policy.

6.5 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) must be conducted where processing is likely to result in a high risk to individuals, including:
· Introduction of new systems or technologies
· Monitoring of employee activity
· Processing of special category data at scale

DPIAs must be reviewed and approved prior to implementation.

7 Individual Rights

Under UK GDPR, you have rights including:

- Access to your personal data.
- Correction of inaccurate or incomplete data.
- Deletion or anonymisation of data ('Right to be Forgotten').

- Restriction or objection to processing.
- Data portability.
- Right to lodge complaints with the ICO.

8 Sharing your personal data

8.1. We may share your data with:

- Payroll providers.
- Pension providers.
- Training or regulatory bodies.
- DBS and vetting agencies.
- Law enforcement (where required).
- IT and security providers supporting ISMS implementation.

8.2. We do not routinely transfer data outside the UK. If necessary, we ensure adequate protections such as standard contractual clauses.

All third-party processors must:
· Be subject to a written data processing agreement
· Demonstrate compliance with UK GDPR
· Implement appropriate security measures aligned to organisational standards

Where personal data is transferred outside the UK, appropriate safeguards will be implemented, including standard contractual clauses or adequacy regulations.

9 Roles and Responsibilities

· The Board of Directors and Senior Managers are responsible for data governance and oversight
· The Data Protection Lead / DPO is responsible for compliance, advice, and subject access requests
· IT and system owners are responsible for technical security controls
· Employees must ensure data is handled responsibly, report breaches immediately, and complete all required training.

10 How to deal with data breaches

All data breaches, near misses, or security incidents must be reported immediately.

The organisation will:
· Contain and assess the breach
· Record the incident in an incident log
· Investigate root causes
· Implement corrective actions

Serious incidents may be reported to the ICO within 72 hours in accordance with UK GDPR.

11 Policy Review

This policy will be reviewed annually or in response to changes in legislation or operational requirements. It does not form part of your employment contract but sets out binding expectations.

12 History of Policy Changes

Date	Page	Details of the change	Agreed by
11/06/2018	All	New Policy – replaces previous Data Protection Policy	Board
Nov 2020	All	2020 Policy Refresh (Good Work April 2020)	Board
Jan 2022	1 & 13	Updated to reflect the new UK GDPR	Board
Jan 23		No change	Board
April 24		No change	Board
April 25		Policy Refresh taking into account ISO 27001 implementation.	Board April 25
May 26		Introduced alignment with Information Security Management System (ISMS) and data classification framework. Strengthened data security section to include RBAC, MFA, encryption, and system controls. Added requirement for audit logging and monitoring of personal data access. Introduced Data Protection Impact Assessment (DPIA) requirements. Clarified employee monitoring and transparency obligations.	Board May 26

		Strengthened third-party data sharing and processor requirements. Expanded international data transfer safeguards. Enhanced data breach response procedures. Clarified organisational roles and responsibilities for data protection	

Appendix 1

The following supporting information is available in the EAT That Frog ISMS system available on the following URL to registered users

1	ISMS Risk Register	
2	Asset Register	
3	Incident/Breach Log	
4	Access Review Reports	
5	Internal Audit Reports	
6	Supplier Confidentiality Agreements	
7	Management Review Minutes	
8	Corrective Action Tracker	
9	Data Retention & Disposal Logs	

https://eatthatfrog.isms.online/login#homepage_vc_tour