

BEYONDLY

G-31

Anti-Fraud Policy

Anti-Fraud Policy

Purpose

In line with our company values, Beyondly is committed to acting responsibly and with integrity and transparency in everything we do. We have a zero-tolerance policy against fraud and are committed to preventing, identifying, and responding to fraudulent activity across all areas of our business.

This policy sits within Beyondly's wider governance framework and should be read alongside all relevant policies and procedures in force, including (but not limited to) our policies around Information Security, Anti-Bribery, Whistleblowing, Financial Processes and Procedures, Employee Competencies framework, and our Code of Conduct.

Scope

This policy applies to:

- All Beyondly employees
- All third parties acting on behalf of Beyondly, including suppliers and partners
- All Beyondly activities, processes, information and assets

Definition of Fraud

Fraud is any deliberate act of dishonesty or deception intended to gain an unfair or unlawful benefit, or to cause loss or harm to Beyondly or others.

This may include (but is not limited to):

- Theft or misuse of funds, assets, or information
- False or inflated expense or payroll claims
- Manipulation or falsification of records
- Procurement or supplier-related fraud
- Misuse of Beyondly systems or data, including cyber-enabled fraud

Roles and Responsibilities

All Employees

- Act in line with Beyondly's values, policies, and codes of conduct
- Follow defined procedures and controls
- Remain alert to potential fraud risks
- Report concerns promptly and in good faith to a member of the SMT



Process number

Leaders and Managers

Process title

- Promote awareness of fraud risks and this policy
- Review fraud risks and ensure appropriate controls are in place
- Escalate and address concerns without delay

All Personnel and Representatives

- Act in line with Beyondly's Supplier Code of Conduct
- Follow defined procedures and controls
- Comply with applicable contractual and ethical requirements
- Remain alert to potential fraud and report concerns

Risk Management and Controls

Fraud risks are identified and managed through:

- Our risk assessments and process reviews
- Defined financial, operational, and information security controls
- Segregation of duties and approval mechanisms
- Supplier and third-party expectations and due diligence
- Secure management of information and systems

Controls are reviewed at least annually to ensure they remain effective and proportionate to risk.

Reporting and Incident Management

Any suspected or actual fraud must be reported to a member of the SMT without delay, or through the channels set out in the Whistle-blowers Policy.

Where fraud is suspected or confirmed:

- Appropriate investigations will be carried out
- Action will be taken to address the incident and prevent recurrence

This may include disciplinary action, terminating contracts, or reporting the matter to external authorities where necessary.

Outcomes are reviewed to support learning and continual improvement.

Awareness and Competence

Beyondly ensures that relevant personnel are aware of this policy and their responsibilities through communication, training, and defined competencies appropriate to their role.

Beyondly aims to have 0% financial loss to fraud

Issue Number: 01

Issue Date: 07/01/2026

Date Last Reviewed: 07/01/2026

Issued by (Name): Jessica Aldersley

Issued by (Signature):



Position: Director

