Safety-Zone Ltd - Data Protection Policy

1. Policy Statement

Safety-Zone Ltd is committed to protecting the privacy and rights of everyone whose personal data we handle. We comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA), which received Royal Assent on 19 June 2025. Some DUAA provisions are being phased in through secondary legislation, and we will update our practices as the Information Commissioner's Office (ICO) publishes further guidance.

We believe that lawful, fair, and respectful treatment of personal data is essential to good working relationships and to maintaining the confidence of those we support. We treat all individuals fairly and respectfully, regardless of age, disability, gender, ethnicity, religion, or sexual orientation.

2. Scope

This policy applies to all staff, contractors, and volunteers who process personal data on behalf of Safety-Zone Ltd. It covers data relating to students, service users, suppliers, and other stakeholders.

3. Data Controller

Safety-Zone Ltd is the Data Controller. We determine why and how personal data is processed. We are registered with the ICO and pay the data protection fee as required under the Data Protection (Charges and Information) Regulations 2018.

4. Lawful Basis for Processing

We process personal data under one or more of the following lawful bases:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Where consent is used, it will be informed, specific, freely given, and recorded.

5. Data Protection Principles

We adhere to the seven principles of UK GDPR:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

6. Data Subject Rights

Individuals have the right to:

- Be informed about data processing
- Access their personal data
- Rectify inaccurate data
- Erase data ("right to be forgotten")
- Restrict processing
- Data portability
- Object to processing
- Challenge automated decision-making and profiling

Requests will be handled **within one calendar month**.

Note: Data breaches must be reported to the ICO within 72 hours of becoming aware of the breach, as required by UK GDPR.

DUAA update: The DUAA introduces changes to automated decision-making and digital verification services. We will update our processes as further ICO guidance becomes available.

7. Data Sharing and Disclosure

We may share personal data with:

- Local authorities
- Funding bodies
- Partner organisations
- Legal and regulatory bodies

Where possible, individuals will be informed of such disclosures. In exceptional cases, data may be shared without consent when required by law or to protect vital interests.

8. International Transfers

Personal data will not be transferred outside the UK unless appropriate safeguards are in place, such as adequacy decisions, standard contractual clauses, or binding corporate rules.

9. Data Collection and Consent

We ensure individuals understand:

- Why their data is collected
- How it will be used
- Who it may be shared with
- Their rights and choices

Consent will be obtained where required and recorded appropriately. We collect only the data necessary for our operational and legal needs.

10. Data Storage and Security

Personal data is stored securely using appropriate technical and organisational measures. Access is restricted to authorised personnel. Data is retained only as long as necessary and securely disposed of when no longer required.

We ensure that any computer systems passed on or sold are wiped of all personal and company data to prevent recovery.

11. Data Breaches

All staff must report suspected data breaches immediately. We will investigate, mitigate, and notify the ICO **within 72 hours** and affected individuals where required.

12. Roles and Responsibilities

- A designated **Data Protection Officer (DPO)** oversees compliance
- All staff receive regular data protection training
- Everyone handling personal data must follow this policy
- Non-compliance may result in disciplinary action

13. Policy Review

This policy is reviewed **bi-annually** and whenever significant changes occur in legislation or operations. Updates will reflect best practice in data management, security, and control.

SIGNATURE:	Robin Clark	**NAME:**	**ROBIN CLARK**
	Managing Director	**DATE:**	**January 2026**

References

- Legislation.gov.uk – Full DUAA Act

https://www.legislation.gov.uk/ukpga/2025/18/introduction/2025-12-01/data.htm

- UK Parliament – DUAA Bill Passage & Documents

https://bills.parliament.uk/bills/3825

- GOV.UK – DUAA Government Collection & Guidance

https://www.gov.uk/government/collections/data-use-and-access-act-2025

- Legislation.gov.uk – Data Protection Act 2018

https://www.legislation.gov.uk/ukpga/2018/12/contents

- ICO – DPA 2018 Overview

https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-protection-act-2018/