



DATA GOVERNANCE POLICY

This applies to the Director and associated persons of EDGEdesign Ltd.

1 Policy Statement

1.1 This policy establishes how the practice governs, manages, protects, and uses data in accordance with:

- CIAT Code of Conduct (2024)
- UK GDPR & Data Protection Act 2018
- ISO 19650 information management principles
- ISO 27001-aligned information security controls
- Professional obligations relating to competence, confidentiality, and duty of care

The purpose is to ensure that all project, client, employee, and organisational data is accurate, secure, ethically managed, and fit for professional use.

2 Governance Principles

2.1 The practice adopts the following principles:

- Professional Integrity — Data handling must uphold CIAT ethical standards
- Confidentiality — Client and project information must be protected at all times
- Competence — Staff must be trained and competent in data handling
- Accountability — Clear ownership of data assets and decisions
- Accuracy — Data must be reliable for design, compliance, and decision-making
- Security by Design — Data protection embedded into workflows
- Transparency — Documented audit trails



3 Responsibilities

3.1 The Director is responsible for:

- ultimate accountability for data governance, compliance, and risk
- overseeing GDPR compliance, DPIAs, breach reporting
- maintaining metadata, quality, naming conventions, CDE standards
- implementing security controls, backups, access management
- maintaining confidentiality, report incidents

4 Data Classification

4.1 The practice classifies data as:

- Public — Marketing materials, published reports
- Internal — Policies, procedures, internal communications
- Confidential — Client data, project information, BIM models, tenders
- Highly Confidential — HR data, financial records, sensitive personal data

Classification determines access, retention, and security controls.

5 Data Quality Standards

5.1 Data must be:

- accurate and validated
- complete and traceable
- consistent with naming conventions
- timely and up to date
- documented with metadata

Quality issues must be logged and resolved through a defined workflow.

6 Access Control & Security

- Access granted on a least-privilege basis
- Multifactor Authentication required for sensitive systems
- BIM models stored in a secure CDE
- Remote access permitted only through secure, monitored channels



7 Privacy & GDPR Compliance

7.1 The practice must:

- maintain a lawful basis for processing
- provide transparent privacy notices
- uphold data subject rights
- report high-risk breaches to the ICO within 72 hours

8 Data Retention & Disposal

- Project data retained in line with PI insurance requirements (typically 6-12 years)
- Secure disposal required for all media (digital and physical)
- Files and BIM models archived where appropriate

9 Data Sharing & Third-Party Management

- External sharing requires a Data Sharing Agreement
- Consultants must meet CIAT-aligned security standards
- CDE access must be controlled, logged, and monitored
- Cloud providers must meet UK GDPR requirements

10 BIM, CDE & Information Management

- All BIM data must follow naming, metadata, and workflow rules
- CDE must maintain version control, audit trails, and permissions
- The Director must oversee data quality and compliance

11 AI, Automation & Digital Tools

- AI tools must use validated, high-quality data
- Outputs must be reviewed by competent professionals
- AI decisions must be explainable where required
- Training data must not include confidential client information



12 Incident Management

- All incidents reported within 24 hours
- Breaches assessed using a standard risk matrix
- ICO notification within 72 hours where required
- Root-cause analysis and corrective actions mandatory

13 Training & Competence

- Mandatory annual data governance training
- BIM and CDE training aligned with ISO 19650
- GDPR refresher training every two years

14 Monitoring, Audit & Review

- Annual internal audits
- Policy reviewed annually or after regulatory changes

Please contact the Director, Dale Webster, if you wish to discuss any issue that is covered by this policy. EDGEidesign Ltd reserves the right to change this policy prior to the review date where exceptional circumstances apply.

The Director of EDGEidesign Ltd approved this policy on the 10th September 2025.

Signed:

A handwritten signature in black ink that reads "Dale Webster". The signature is written in a cursive style and is positioned above a horizontal line.

Dale Webster, Director
(Signed on behalf of EDGEidesign Ltd)

Next review date: September 2026