
| BCTG Data Protection Policy | |
|---|---|
| **Reviewed by** | **Nick Holland** |
| **SLT Signature** | **A.Hackett** |
| **Advisory Board sign off by** | **Alan Phillips** |
| **Signature** | **A.Phillips** |
| **Date** | **February 2025** |
| **Review date** | **February 2026** |

# Data Protection Policy

## 1. Introduction

BCTG is committed to ensuring the privacy, security, and proper handling of personal data in accordance with the General Data Protection Regulation (GDPR) and other relevant data protection laws. This policy sets out the organisation's approach to data protection, ensuring compliance and mitigating risks associated with data breaches.

## 2. Policy Aim

The aims of this policy are to ensure that all staff, service users and stakeholders:

- Understand how personal data should be processed.
- Comply with all applicable data protection laws and best practices.
- Protect BCTG from risks associated with personal data breaches and regulatory non-compliance.

## 3. Principles of Data Protection

BCTG is committed to processing personal data in line with the following principles:

- **Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation:** Data shall only be collected for specified, legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimisation:** Only data that is necessary for the intended purpose shall be collected and processed.
- **Accuracy:** Personal data shall be kept accurate and up to date.
- **Storage Limitation:** Data shall not be retained for longer than necessary and shall be securely disposed of when no longer required.
- **Integrity and Confidentiality:** Data shall be processed securely to prevent unauthorised or unlawful access, loss, destruction, or damage.
- **Accountability:** BCTG shall be responsible for demonstrating compliance with data protection principles.

## 4. Data Processing and Management

### 4.1. Responsibilities

- **Data Protection Officer (DPO):** Ensures compliance with GDPR and oversees data protection activities.
- **All Staff:** Must adhere to this policy, complete relevant training, and report any suspected data breaches.

### 4.2. Security Measures

- Paper records containing personal data shall be stored in a secure environment with restricted access.
- Digital data shall be protected by strong passwords, encryption, and access controls.
- Personal data shall not be shared externally without proper authorisation.
- Confidential information shall never be left unattended or discussed outside authorised personnel.

### 4.3 Data Breach Management

- Any suspected or actual data breaches must be reported immediately to the DPO.
- The DPO will assess the breach, implement corrective actions, and report to relevant authorities if necessary.
- Affected individuals will be notified in compliance with GDPR requirements.

### 5. Data Retention and Disposal

- Personal data shall be retained only as long as necessary in accordance with the **Document Storage, Retention, and Disposal Policy**.
- Secure disposal methods (e.g., shredding, permanent deletion) shall be used for obsolete records.

### 6. Staff Training and Compliance

- Regular data protection training shall be provided to all employees handling personal data.
- Staff must acknowledge their understanding and compliance with data protection requirements.
- Non-compliance may result in disciplinary action.

### 7. Policy Review and Updates

This policy will be reviewed annually or sooner if required by regulatory changes. The Advisory Board is responsible for approving amendments to ensure continued compliance.

### Policy Review

This policy will be reviewed on an annual basis by the BCTG Advisory Board.