



# Data BELTANE COLLEGE

## Protection Policy

Member Responsible for Policy		Ben Swallow <b>Director of Business and Finance</b>	
Version	One	Last Updated	July 2025
Approving Directors		R. Bromley-Woods, D Pheasey, J. Booth	
Date of Next Review		July 2026	

## Introduction

Beltane College is committed to providing holistic education and wellbeing, of the highest quality and this policy is underpinned by the college culture and values.

**Confidence**– We are enthusiastic, we act authentically and with purpose

**Fairness** – Showing care through our interactions and tackling inequalities

**Integrity** – We are honest, trustworthy and dependable; we do what we say we will do

**Teamwork** – We achieve more together and remain mindful of everyone’s wellbeing.

## Policy intent and scope

The College is committed to conducting its operations in full compliance with all applicable data protection legislation and in adherence to the highest standards of ethical practice.

This policy governs the processing of personal data held in both manual and electronic records maintained by the College. It also outlines the College’s approach to:

- Responding to data breaches.
- Upholding the rights of individuals under UK GDPR and the Data Protection Act 2018.

## Audit and Governance

To ensure the implementation of this policy the College has designated the Director of Business and Finance as the College’s Data Protection Officer. All enquiries relating to the holding of personal data should be referred to the Data Protection Officer in the first instance.

## Policy Accessibility and Communication

To promote awareness and compliance, this policy will be:

- **Published** on the College’s official website.
- **Provided** to all new team members as part of the induction process.

## General Statement on Data Collection and Use

The College collects and processes personal data about staff, students, and others to fulfil:

- Contractual obligations (e.g. payroll, absence recording)
- Legal duties (e.g. tax, statutory benefits)
- Educational responsibilities (e.g. student welfare and safeguarding)

Where appropriate, data may also be processed for legitimate interests such as equality monitoring—ensuring anonymisation where possible.

The College is committed to:

- Transparency about data collection and sharing
- Ensuring accuracy, relevance, and secure storage
- Retaining data only as long as necessary
- Responding to Subject Access Requests in line with UK GDPR
- Making sure all team members understand their responsibilities

## **Individual Rights Under UK GDPR**

Individuals have the right to:

- Be informed about the use of their data
- Access, correct, or request deletion of their data
- Restrict or object to processing (where permitted)
- Withdraw consent (if applicable)
- Challenge automated decisions and lodge complaints with the ICO

Rights may be limited when data is processed for legal obligations, public interest, contracts, or vital interests.

Data will be processed only when lawful grounds apply, including consent, contract performance, legal obligations, protection of vital interests, public duties, or legitimate interests.

## **Data Security and Breach Management**

### **Responsibilities:**

Staff members must:

- Keep data secure (digital and paper-based)
- Avoid unauthorised disclosure
- Open confidential communications only if addressed to them
- Use College addresses and emails for work only

### **Breaches Include:**

- Unauthorised access or disclosure

- Data sent to the wrong recipient
- Lost or stolen devices
- Unlawful data changes or loss of access

## **Reporting and Response:**

- Report suspected breaches immediately to the DPO
- Submit a breach report—do not investigate independently
- The DPO will assess, record, and notify the ICO within 72 hours (if required)
- Affected individuals will be informed, and prevention measures applied

## **Subject Access Requests**

Requests should be made in writing to the Data Protection Officer and include:

- Name, contact details, and identifying information
- Clear scope and timeframe of the data requested
- Preferred method of receiving the response

Requests will be verified through appropriate ID and responded to within **30 calendar days**. Where data is redacted, a full record will be retained. All disclosures must be clear and legible, with any codes or terms explained.

## **Training and Support**

All relevant personnel will receive data privacy training. For further information, contact the [Information Commissioner's Office \(ICO\)](#) or call **0303 123 1113**

## **Actioning a subject access request**

### **Access, Correction, and Erasure of Personal Data**

Individuals have the right to access their personal data without charge by submitting a written request to the Data Protection Officer. Responses are provided within one month, extendable by two months for complex or numerous requests. Unfounded, excessive, or repetitive requests may be refused or incur a reasonable fee.

Individuals may also request correction or deletion of data that is inaccurate or no longer necessary. The College will assess whether there is a legitimate reason to retain the data and will inform the individual if no action is taken. If dissatisfied, individuals may contact the UK's supervisory authority—the Information Commissioner's Office (ICO).

Where data is corrected, relevant third parties (e.g. HMRC) will be notified as appropriate.

Requests for information must be made in writing; which includes email and be addressed to the Data Protection Officer.

The request should include:

- 'Subject access request' as your email subject line or a heading for your letter
- the date of your request
- your name (including any aliases, if relevant)
- any other information used by The College to identify or distinguish you from other individuals
- your up-to-date contact details
- a comprehensive list of what personal data you want to access, based on what you need
- any details, relevant dates, or search criteria that will help the College identify what you want
- how you would like to receive the information

If the initial request does not clearly identify the information required, then further enquiries will be made.

The identity of the requestor must be established before the disclosure of any information. Evidence of identity will be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

*This list is not exhaustive.*

Any individual has the right of access to information held about them. The response time for subject access requests, once officially received, is 30 calendar days.

The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

## **Training**

The College will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Further advice and information is available from the Information Commissioner's Office, [Information Commissioner's Office \(ICO\)](#) or telephone 0303 123 1113

## **Related Legislation**

*Data Protection Act 2018*

*UK General Data Protection Regulation (UK GDPR)*

*Information Commissioner's Office (ICO) Codes of Practice*