Burton and South Derbyshire College

Creating the skills of tomorrow.

Record/Data Management & Retention Policy

www.bsdc.ac.uk

Policy Title	
Policy Summary	This Retention/Data Retention Policy sets out details of the policies for the retention of special categories of personal data.
Policy Owner	Deputy Principal (DPO)
Policy Version	V3.1
Approved By	Senior Leadership Team (SLT)
Date Approved	February 2025
Distribution	Internal & External (Published)
Equality Impact Assessment	Completed February 2025
Linked Policy/Documents	
Data Protection Policy Rights of Individuals Policy College-Wide Privacy Notice	

Contents

Policy Definitions 3

(1) **Policy Overview** 3

(2) **Scope** 4

(3) **Compliance and Monitoring** 4

(4) **Data/Information Disposal & Erasures** 4

(5) **Record/Data Retention Periods (Retention Schedule)** 5

(6) **Data Back-ups** 6

EQUALITY IMPACT ASSESSMENT (EIA) 7

Policy Definitions

The College	Burton & South Derbyshire College (BSDC)
Data Protection Officer (DPO)	Burton & South Derbyshire College (BSDC) Data Protection Officer: DP.Officer@bsdc.ac.uk 01283 494400
BSDC Personnel	Any college employee, who accesses any of the College's Personal Data and will include consultants, contractors, and temporary personnel hired to work on behalf of the College.
Data Controller	Any entity (e.g. company, organisation, or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws.
Data Protection Laws	The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'
Individuals	Living individuals who can be identified, *directly or indirectly*, from information that the College has.
Personal Data	Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.
Processor	Any entity (e.g. company, organisation, or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a Controller.
Special Categories of Personal Data	Personal Data that reveals a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological, or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

(1) Policy Overview

a) Burton & South Derbyshire College (BSDC) must, in respect of its processing of personal data, comply with the Data Protection Act, the General Data Protection Regulation (GDPR).

b) BSDC is committed to establishing and maintaining good data management to ensure that it retains important information while also ensuring that data no longer required is disposed of in line with its obligations under data protection legislation.

c) BSDC's *Data Management & Retention Policy* should be read in conjunction with BSDC's Data Protection Policy, which sets out the organisations overall approach to data protection and management.

d) BSDC is under a legal obligation only to keep personal data for as long as necessary for legitimate purposes including those mandated by its regulators and funding agencies. Once BSDC no longer requires the personal data, it will be safely and securely destroyed.

e) Overall accountability for the management and retention of BSDC's data rests with the Principal and Chief Executive Officer (CEO). The responsibilities for the oversight of receiving, controlling, processing, handling and deletion of data are delegated and overseen by BSDC's appointed Data Protection Officer (DPO).

f) All BSDC's personnel are responsible to the DPO for ensuring that records/data containing personal identifiable information created in the course of its business functions are proportionate, appropriate, accurate, up-to-date and securely maintained in accordance with general data protection regulations and BSDC's *Data Protection Policy*.

g) This Policy applies to all BSDC personnel, inclusive of, but not limited to employees, consultants, contractors and temporary personnel hired to work on behalf of BSDC. All BSDC personnel with access to personal data must also comply at all times with GDPR legislation, BSDC's Data Protection Policy and a failure to do so will be treated seriously and may result in disciplinary action for the individual.

(2) Scope

a. In accordance with data protection law, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data. BSDC's methods and measures for destroying and erasing data are noted in this policy and apply to all forms of personal data.
b. This policy applies to all personal identifiable data (both physical and digital) which is, received, processed, retained, shared (with consent) and destroyed in the course of BSDC's business functions.

(3) Compliance and Monitoring

a. BSDC is committed to ensuring the continued compliance with this policy and any associated legislation and undertakes regular reviews, audits and monitoring of records, their management, archiving and their retention. Information asset owners are tasked with ensuring the continued compliance and review of data within their remit which includes:

- Data is appropriately recorded and where necessary indexed for future retrieval
- Oversee procedures for keeping the system and information updated
- Provide appropriate training for those individuals receiving, handling, disposing of data/information
- Ensuring secure storage facilities, with controlled secure access

(4) Data/Information Disposal & Erasures

a. BSDC continuously reviews the types of personal data it holds and the purposes for which it is used. The table in section 5, outlines the retention periods set by BSDC for its various asset owners and the data types they hold.
b. All data authorised for disposal must be destroyed in as secure a manner as is necessary for the level of confidentiality or security they merit and in accordance with GDPR and the *College Data Protection Policy*. This applies to electronic as well as physical data.
c. In specific circumstances, a data subject has the right to request that their personal data is erased. However, BSDC recognises that the 'right to be forgotten' is not absolute. The right to have personal data erased and to prevent processing only applies:
    - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
    - When the individual withdraws consent (when the personal data is collected under this lawful basis)
    - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
    - The personal data was unlawfully processed.
    - The personal data must be erased to comply with a legal obligation.
    - The personal data is processed in relation to the offer of information society services to a child.

d. Where BSDC receives a request to erase data the first step will be to determine which data set the right of erasure applies to, if any. If the right does apply, the erasure will be carried out under instructions of the DPO in conjunction with the relevant department/individual to ensure that all data relating to that individual has been erased.

e. Erasure should take place within 1 calendar month of the request being received. Where BSDC is unable to act in response to a request for erasure, a written explanation will be provided to the individual and inform them of their right to complain to the Information Commissioners Office (ICO).

(5) Record/Data Retention Periods (Retention Schedule)

Asset Owners	Record Type/Classification	Short 1 year	Medium 3 yrs. + Current	Long 6 yrs. + Current	Special Durations
General	CCTV Security				30 days.
	Data Subject Requests Freedom of Information Requests Data Erasure (Request Only)		✓		
	Email Correspondence		✓		
	Visitor Records				1 wk.
Governance	Agendas, Papers and Records of the Corporation				12 yrs.
	Minutes of Corporation Inc. Committees				Permanently
	Minutes of College Committee Meetings			✓	
	Quality Records (Inc. Audits)		✓		
Curriculum & Quality	Learners References & (Inc. UCAS Records / References)		✓		
	Learner / Apprentice DBS Records		✓		
	Tutor Utilisation Workload Agreements		✓		
	Learner & Apprentice Assessment Records		✓		
	Internal Quality Assurance Records		✓		
Services for Learners	Learner Pastoral Records Inc. medical protocols, ALS, EHCP)			✓	
	Complaints & Compliments Records			✓	
	Child Protection and Safeguarding Records				Permanently
	Library Registry Records		✓		
Registry & Exams	Learner Record Inc. Attendance Data			✓	
	Examination / Qualifications Results			✓	
	Enrolment Records			✓	
	Enrolment Records (ESF)				10years
Finance	Financial Transactions			✓	
	Expenses Claims			✓	
	Internal & External Audits			✓	
	Payroll Information			✓	
	Public Liability Certificates		✓		
	Employer Liability Certificates				40 yrs.
	Legal Claims & Disputes		✓		
Estates & Facilities	Accidents & Incident Reports				3 yrs.
	Accidents & Incident Reports (Health and/or Environment)				40 yrs.
	Educational Visits Records		✓		
People & Performance	Personal File Records			✓	
	Recruitment & Selection Records	✓			
	Work Related Illness / Injury Records				40 yrs.
	Payroll Records			✓	
	Pension Records				75 yrs.

N.B Where data does not fall within the various categories set out in the retention schedule, advice should be sought from BSDC's DPO.

(6) Data Back-ups

a. When digital data is deleted from the College's "live systems" in accordance with the defined periods outlined in section 5 of this policy or following an erasure request. This data will remain within the College's secure backups, which are beyond normal use and accessibility, for a further 12 months, after which it will be securely overwritten.

EQUALITY IMPACT ASSESSMENT (EIA)	
Please ensure that you have read the Equality Impact Assessment guidance document before completing this form.	
Stage 1: Identify the Policy, Procedure or Practice	
Name of policy, procedure or practice	Record Management & Retention Policy
Owner of policy, procedure or practice	Deputy Principal
Status of policy, procedure or practice	Active
Accessibility of policy, procedure or practice	All
Stage 2: Description of Policy, Procedure or Practice	
What are the main aims of the policy, procedure or practice?	
This Retention/Data Retention Policy sets out details of the policies for the retention of special categories of personal data.	
Who does the policy, procedure or practice cover?	All data subjects College personnel
How often is this policy, procedure or practice reviewed?	Every 3 years – Updated accordingly.

Stage 3: Implications for a Protected Characteristic Group

Is there a potential implication or barrier for a protected characteristic group?

	YES/NO	What is the implication / Barrier?	
Age	NO		Go to Stage 4
Disability	NO		
Ethnicity	NO		
Gender	NO		
Gender Re-Assignment	NO		
Marriage / Civil Partnership	NO		
Pregnancy / Maternity	NO		
Religion / Belief	NO		
Sexual Orientation	NO		

	Tick	
No potential implications or barriers exist for a protected characteristic group associated with this policy, procedure, or practice.	✓	7 G TO Stage

Stage 4: Protected Characteristic Group Implications Evidence Base

What evidence do you have for the conclusion of a potential implication or barrier for a protected characteristic group? **(none or comment)**

None

What impact does this evidence show?	**Tick**	
Positive Impact		Go to Stage 7
Negative Impact		Go to Stage 5
No Impact	✓	Go to Stage 7

Stage 5: Involve and Consult Stakeholders to Address any Negative Impacts	
Please provide brief details of involvements and consultations undertaken to address negative impacts **(none or comment)**	Go to Stage 6
None	
Stage 6: Consultation Enforced Changes	
Outline any changes made to the policy, procedure, or practice as a result of consultations with stakeholders **(none or comment)**	Go to Stage 7
None	
Stage 7: Published Results	
Once completed, this policy, procedure or practice and EIA and any relevant supporting information should be submitted to CMT/SLT for approval and inclusion on CollegeiP. Please list all supporting documents submitted with this assessment here:	

Signing Off Process	
Name of Staff Completing E.I.A	Phillippa Kendrick
Signature	P.Kendrick
Date Completed	10/02/2025