Data Protection Policy

Policy Title	**Data Protection Policy**
Issue Date	December 2024
Author	Olivier Cognard, Vice Principal of Funding, Planning and System Improvements
Approved by	Corporation Board, December 2024
In consultation with	Audit Committee and SMT
Review date	December 2027
Issue Number	3
Equality Impact Assessment	08/11/24

1. Introduction

The General Data Protection Regulations (‘GDPR’) regulates how organisations use the personal data of living individuals. It requires organisations to be accountable and transparent in its handling of such data and gives individuals rights to challenge its use and to access the data held.

2. Definitions

2.1 For the purpose of this policy the term **‘staff’** shall encompass staff, volunteers, self-employed workers, sub-contractors and PGCE students.

2.2 The term **‘personal data’** covers two categories of data:

Personal – Any information relating to an identifiable person such as name, contact details, date of birth, photos, location data or online identifier (such as IP address).
Sensitive – Special category data about the individual relating to race, ethnicity, sex life, sexual orientation, politics, religion, health, trade union, criminal convictions, genetic and biometric data.

For this policy personal and sensitive data are collectively called ‘personal data’.

2.3 An individual to whom personal data relates is called a ‘**Data Subject’.**

2.4 **‘Processing’** is anything that is done with personal data, including collection, storage, use, disclosure, and deletion.

2.5 We consider personal data **‘breach’** incidents and have a reporting mechanism that is communicated to staff. We assess whether we need to report breaches to the ICO and we take appropriate action to make data subjects aware if needed. (See Data Breach Procedure)

3. College responsibilities and compliance

3.1 Responsibilities

Under the GDPR regulations the college is required to put in place comprehensive but proportionate governance measures to minimise the risk of data breaches (to be communicated to the Data Protection Officer – dpo@abingdon-witney.ac.uk) and to uphold the protection of personal data.

Specifically, the college must comply with the principles governing the use of personal data and must ensure that data is:

3.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

3.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and only the minimum amount of personal data necessary for the intended purpose is collected and processed;

3.1.4 accurate and, where necessary, kept up to date;

3.1.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

3.1.6 processed in a manner that ensures appropriate security of personal data.

3.2 Compliance

In order to ensure full and effective compliance with its data protection responsibilities, the college:

3.2.1 nominates both a Data Protection Officer (DPO) and a Deputy Data Protection Officer (DDPO)

3.2.2 adopts a robust approach to data security, including:

- ensuring that specific physical and electronic spaces are made available for the storage of personal data
- prohibiting the transfer of personal data to external devices, unless approved by the DPO under an appropriate data sharing agreement
- ensuring that all staff report any breaches of data security
- ensuring appropriate precautions are taken when using mobile devices
- ensuring that all requests to share personal data with third parties are referred to the DPO for approval. The DPO will also provide advice about secure and appropriate methods of sharing data if appropriate.

3.2.3 follows a clear Data Retention Procedure that outlines what personal data is kept, why it is kept, how it is kept and for how long

3.2.4 maintains records of data processing activities.

3.2.5 publishes a Privacy Statement outlining:

- The organisation and contact details of the DPO
- The basis for collecting personal data
- How the personal data is used
- How it is kept secure

3.2.6 respects, facilitates and appropriately responds to the rights of Data Subjects, including by:

- seeking consent to use personal data (if required), ensuring that this consent is of an “opt in” nature
- providing access to a copy of personal data and supplementary information in either hard copy or electronic format, within a month of a formal request being made
- rectifying any inaccuracies or incomplete personal data within a month of a formal request being made
- erasing all personal data if it is not required to be kept for a legitimate need within a month of a formal request being made
- notifying Data Subjects if the security of their personal data is compromised within 14 days of a breach occurring
- complying with a withdrawal of consent within a month of the request being made
- disclosing any automated decision making / profiling practices

The Data Subject Request form is made available via the college website or by request from the college Data Protection Officer.

3.2.7 Carries out Privacy Impact Assessments on all new projects and on significant changes to existing projects that involves personal data processing to help identifying and mitigating potential privacy risks at an early stage.

3.2.8 Ensures that all staff are fully trained in respect of their data protection responsibilities

3.2.9 Records and responds to actual or potential data protection compliance failures effectively. Staff are required to report any actual or potential breaches to the DPO who will:

- Report any data breach where there are significant risks to people's rights and freedoms to the ICO as soon as possible but within 72 hours
- Take remedial action to mitigate the situation
- Notify individuals affected by the breach
- Maintain a log of actual and potential compliance failures

4. Specific Responsibilities

All staff must comply with this policy and all guidance, procedures and protocols relating to it. Specific staff responsibilities:

4.1 Governors

As a corporate body, the Governors have overall responsibility to ensure comprehensive governance measures are in place to minimise the risk of data breaches and to ensure policy documents are reviewed on a regular basis.

4.2 **College Leadership Team** (CLT)

The CLT to:

- Ensure compliance of college data protection practices within their respective areas of work
- Ensure all staff within their area of work complete annual training / refresher
- Liaise with the DPO in relation to new projects to ensure Privacy Impact Assessment are undertaken
- Regular review of compliance issues at CLT meetings.

4.3 Data Protection Officer

- Through the Business Improvement Committee keep CLT/ SMT updated on data protection responsibilities, risks and issues
- Manage all compliance audit activities
- Manage the Information Asset Register
- Manage the Privacy Impact Assessment process
- First point of contact for all staff in relation to data protection queries
- Manage data subject request process and breach incidents

4.4 Head of People Services

- Ensure recruitment / employment / induction practices raise awareness of data protection legislation and employee obligations in relation to compliance
- Ensure applicants and staff are made aware of how their personal data is used
- Work with Head of ITS to ensure suitable training opportunities are offered to staff so they can respond to changes in IT systems and are sufficiently skilled to maintain secure IT practices

4.5 Marketing Manager

- Ensure Privacy Statements are easily accessible on the College website
- Ensure data protection statements attached to emails and other marketing copy is compliant
- With the DPO, manage data protection queries from clients, target audiences or media outlets
- With the DPO, ensure all marketing initiatives are compliant

4.6 Head of Information Services

- Ensure all IT systems and services are compliant in themselves and support compliance by all users
- Ensure all third-party access to software / servers is authorised and recorded
- Work with Head of HR and Head of Digital Learning to ensure suitable training opportunities are offered to staff so they can respond to changes in IT systems and are sufficiently skilled to maintain secure IT practices

4.7 Head of Estates & Capital Development

- Ensure the CCTV system is well maintained and the CCTV policy is fully implemented.

4.8 Head of MIS

- Ensure enrolment practices support students to fully understand how their data is to be used before any paperwork is signed / enrolment completed
- Ensure department practices and procedures comply fully with data protection legislation and give maximum opportunity for data to be recorded accurately

5. Document and data retention

The rationale for document and data retention at the College is outlined in Appendix 1.

5.1 ESF 2014 – 2020 Programme

Document retention for projects funded under the ESF 2014 – 2020 Programme are also covered under this policy. All project documents will be kept for 10 years after the final ESF claim is paid by the ESF Managing Authority and the Managing Authority will be consulted before record are disposed of.”

6. Further Information

- This policy links to the CCTV Procedure and IT Regulations.
- Data Sharing Procedure
- AW College Data Sharing Agreements
- Data Breach Procedure

Data Breach Incident and Subject Access Request Logs

- Full details of data protection legislation can be access through the Information Commissioner’s Office at www.ico.org.uk.

Overview of Data Retention Practices

Abingdon & Witney College only retains information for the period required for the purpose it was collected. This document gives an overview of Abingdon & Witney College's retention practices in relation to personal data.

Student	Examples	Retention Period	Rationale	Method of Deletion
Course Application (not converting to enrolment)	Application forms Application record	Full time: 3 full academic years Part time: 1 full academic year	To support students with further applications Part of end of year audit	Hardcopy: shredded Database: all data
Enrolment / Funding	Enrolment forms Transfer Withdrawal Bursary info Exams data Attendance Disciplinary	7 years	Funding authority requirement	Hardcopy: shredded Database: all data
Student Support	Safeguarding files Bursary / Financial	Indefinite 7 years	Business needs to safeguard college interests in any future claim. DPO permission required to access.	Not applicable
Health & Safety	Risk Assessments	5 years	HSE requirement	Hardcopy: shredded Electronic: permanently deleted
Complaints	Correspondence with complainants	7 years	Business needs to safeguard college interests in any future claim.	
Accreditation		3 years	Awarding organisation recommendation	Hardcopy: shredded Electronic: permanently deleted
Student work	Portfolio Course work / Projects Progress report	Current Academic year +1		
Financial / Fees	Purchase Ledger Sales Ledger Cash book payments	7 years	Legal requirement	Hardcopy: shredded Database: not applicable

Recruitment/Staff	Examples	Retention Period	Rationale	Method of Deletion
Application		12 months from closure of recruitment campaign except for the person appointed (kept for the duration of employment)	Business needs	Hardcopy: shredded Electronic: permanently deleted
Employment *(including activities such as training, performance, occupational health)*	Training Performance record Occupational Health	7 years	Business needs to safeguard college interests in any future claim. DPO permission required to access.	Hardcopy: shredded Database: permanently deleted
Payroll		3 previous and current	Business needs to safeguard college interests in any future claim. DPO permission required to access.	Hardcopy: shredded Electronic: permanently deleted
Health & Safety		7 years	Business needs to safeguard college interests in any future claim. DPO permission required to access.	Not applicable
Safeguarding	**DBS**	No more than 6 months	Code of Practice requirement	Hardcopy: shredded Electronic: permanently deleted

General	Examples	Retention Period	Rationale	Method of Deletion
Data Protection / FOIA requests	Correspondence regarding Data Protection/ GDPR / FOIA request	7 years	Business needs to safeguard college interests in any future claim.	All emails and related correspondence
Subject Access Request		Infinite		
CCTV		28 days	Automatic deletion (max of 28 days).	

ESF 2014-2020 Programme		10 years / 2030	Project documents will be kept for 10 years after the final claim Not without prior consultation with the managing authority	

			Hardcopy: Shredded Electronic: permanently deleted	
Contractual Arrangements	Service Level Agreement Legal Contracts Tender Documentation Capital/Revenue grant	7 years	Business needs to safeguard college interests in any future claim.	