Data Protection Policy

Version	Date	Changes	Reason for Changes	Author/ Reviewer	Next Review
v2.1	June 2024	Amendments of minor syntax and spelling errors	Annual review was due	Mohammad T Islam (Head of Academics & Quality Control)	June 2025/ As required
v3.1	June 2025	Amendments of minor syntax and spelling errors	Annual review was due	Mohammad T Islam (Head of Academics & Quality Control)	June 2026/ As required

1.0 Purpose

This policy sets out how Commonwealth College of Excellence collects, processes, stores, and protects personal data relating to its staff, students, and other stakeholders, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2.0 Scope

This policy applies to all staff, students, contractors, consultants, and third parties who have access to personal data held by the College, regardless of the medium in which the data is held.

3.0 Definitions

- **Personal data**: Any information relating to an identified or identifiable natural person.
- **Special category data**: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, or data concerning a person's sex life or sexual orientation.
- **Data subject**: The individual to whom the personal data relates.
- **Data controller**: The organisation that determines the purposes and means of processing personal data (i.e. the College).
- **Data processor**: A person or organisation that processes personal data on behalf of the data controller.

4.0 Data Protection Principles

The College adheres to the following principles as set out in the UK GDPR. Personal data shall be:

1. Processed lawfully, fairly, and in a transparent manner.
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than necessary.
6. Processed in a manner that ensures appropriate security of the personal data.

5.0 Lawful Bases for Processing

The College will only process personal data where there is a lawful basis under Article 6 of the UK GDPR. These may include:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public task
- Legitimate interests (except where overridden by the rights of the data subject)

6.0 Rights of Data Subjects

Under the UK GDPR, data subjects have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (the “right to be forgotten”)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Requests to exercise these rights must be made in writing to the Data Protection Officer (DPO). The College will respond within one calendar month, unless an extension is justified.

7.0 Data Security and Storage

The College will implement appropriate technical and organisational measures to secure personal data against unauthorised access, alteration, disclosure, or destruction. These include, but are not limited to:

- Access controls and user authentication
- Encryption and secure file transfer protocols
- Regular security training for staff
- Secure physical storage of hard-copy records
- Regular data audits and risk assessments

8.0 Data Retention

The College will retain personal data only for as long as necessary to fulfil the purposes for which it was collected, including any legal, regulatory, or reporting requirements. Specific retention periods are outlined in the College’s Data Retention Schedule.

9.0 Data Sharing and Transfers

Personal data may be shared with third parties only when necessary and subject to appropriate safeguards.

Where personal data is transferred outside the UK or EEA, the College will ensure that adequate protection is in place in accordance with UK data protection laws.

10.0 Roles and Responsibilities

- **Senior Management** is responsible for overall compliance.
- **The Data Protection Officer (DPO)** oversees data protection strategy, advises on compliance, and is the main contact for data subjects and the Information Commissioner’s Office (ICO).
- **All staff and contractors** must adhere to this policy and complete relevant training.

11.0 Data Breach Management

All data breaches or suspected breaches must be reported immediately to the DPO. The College will investigate and, where required, notify the ICO within 72 hours of becoming aware of a notifiable breach.

12.0 Monitoring and Review

This policy will be reviewed annually or following significant changes in legislation, guidance, or College operations.

The End