Data Protection Policy

CECOS College London
1st Floor,
23 South Mall,
St Georges Chambers,
London,
N9 0TS

Policy Name	Data Protection Policy (GDPR)	Policy Number	V3:5

Effective Date	01/03/2026	Date of Last Revision	01/03/2026	Version Number	3:5

Responsible Officer	Marlon Mason	Contact Email	marlon@cecos.ac.uk

Scope

This policy applies to:

- All staff, including teaching, support, and management staff
- The **Chief Executive, Principal, and Governance Board**
- All current, past, and prospective learners
- Contractors, subcontractors, and external partners
- Any individual processing personal data on behalf of CECOS College

This policy applies to all personal data:

- Held in **electronic or paper formats**, including emails, CCTV, photographs, video, and audio recordings
- Processed for administrative, academic, legal, or operational purposes

Failure to comply with this policy may result in:

- Legal liability for both the College and individuals
- Disciplinary action under College procedures

Policy Statement

CECOS College is committed to protecting the rights and privacy of individuals in accordance with the **UK GDPR and Data Protection Act 2018**.

The College will ensure that personal data is:

- Processed **lawfully, fairly, and transparently**
- Collected for **specified, explicit, and legitimate purposes only**
- **Adequate, relevant, and limited** to what is necessary
- **Accurate and kept up to date**
- **Stored securely** and protected against unauthorised access
- **Retained only as long as necessary**
- Processed in accordance with the **rights of data subjects**

CECOS will:

- Provide clear **privacy notices** at the point of data collection
- Ensure lawful bases are established for all processing
- Apply enhanced controls for **special category (sensitive) data**
- Maintain robust **technical and organisational security measures**
- Ensure staff are trained and aware of their responsibilities

Relevant Legislation

Title	Date
UK General Data Protection Regulation (UK GDPR)	
Data Protection Act	2018
Privacy and Electronic Communications Regulations (PECR)	
Freedom of Information Act	2000
Human Rights Act	1998

Related Policies

Title	Effective Date
Information Security Policy	01/03/2026
Safeguarding & Prevent Policy	01/03/2026
IT Conduct Policy	01/03/2026
Data Breach Procedure	01/03/2026

Version History

Version	Approved By	Revision Date	Details of change
3:5	Hariss Pervez	01/03/2026	Minor revision.

Exceptions

There are no general exceptions to this policy. However:

- Personal data may be processed without consent where:
    - There is a **legal obligation**
    - It is necessary for a **contract**
    - There is a **vital interest** (e.g. safeguarding or risk to life)
    - It is required for **public task or legitimate interest**
- Personal data may be disclosed:
    - To regulatory or law enforcement authorities
    - In emergency situations

All such processing must be:

- Lawful, necessary, and proportionate
- Clearly documented and justified

Additional Comments

Data Protection Principles

CECOS adheres to the following principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy

5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Lawful Basis for Processing

Personal data will only be processed where a lawful basis applies:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Special category data (e.g. health, ethnicity, religion) will only be processed where additional legal conditions are satisfied, including:

- Explicit consent
- Employment or legal obligations
- Vital interests
- Legal proceedings
- Substantial public interest

Data Subject Rights

Individuals have the right to:

- Access their data (Subject Access Request)
- Request rectification of inaccurate data
- Request erasure
- Restrict or object to processing
- Data portability
- Opt out of direct marketing
- Challenge automated decision-making

Requests must be responded to within **one calendar month**.

Data Security

CECOS will implement appropriate safeguards, including:

- Secure IT systems and access controls
- Encryption where appropriate
- Secure storage of physical records
- Staff training and awareness

All staff must report any actual or suspected data breach immediately.

Data Breaches

A data breach includes:

- Loss or theft of personal data

- Unauthorised access or disclosure
- Accidental loss, destruction, or alteration

All breaches must be:

- Reported immediately to the **Data Protection Officer (DPO)**
- Investigated and documented
- Reported to the ICO within **72 hours**, where required

Data Retention and Disposal

- Personal data will not be retained longer than necessary
- Retention periods are defined in the Records Retention Policy
- Data will be securely destroyed when no longer required

Third-Party Processing

- Third parties must comply with GDPR requirements
- Data Processing Agreements (DPAs) must be in place
- Due diligence must be undertaken before sharing data

International Data Transfers

- Personal data will not be transferred outside the UK/EEA unless appropriate safeguards are in place

- The DPO must approve any such transfers

Data Protection Impact Assessments (DPIAs)

A DPIA must be conducted where processing is likely to result in a high risk to individuals, including:

- Use of new or innovative technologies
- Large-scale processing of sensitive data
- Automated decision-making or profiling
- Monitoring of publicly accessible areas
- Data matching or combining datasets
- Processing involving vulnerable individuals

DPIAs:

- Must be completed prior to processing
- Should inform project design and risk mitigation
- Are an ongoing process for managing data protection risks

Governance, Ownership and Accountability

Area	Responsibility	Role
Strategic Oversight	Governance Board	Ensures compliance and effectiveness
Executive Accountability	Chief Executive	Overall accountability

Operational Implementation	Principal	Ensures policy implementation
Policy Ownership	Data Protection Officer (DPO)	Maintains and monitors policy
Operational Support	Senior Managers	Ensure compliance in departments
All Staff	All employees	Responsible for data protection compliance

---

Staff Responsibilities

All staff must:

- Maintain confidentiality of personal data
- Only access data they are authorised to use
- Not disclose personal data without appropriate authorisation
- Follow College procedures and policies
- Complete mandatory data protection training

Managers must:

- Ensure staff understand their responsibilities
- Implement appropriate data management procedures
- Ensure retention and disposal rules are followed

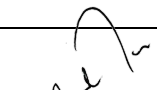
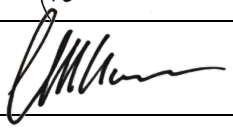
Review Cycle and Version Control

- This policy will be reviewed **annually as a minimum**

- Next scheduled review: **March 2027**
- Earlier review may occur due to:
    - Legislative changes
    - Organisational changes
    - Data breaches or identified risks

Version	Date	Summary of Changes	Next Review
3.4	March 2026	Full revision, governance updates, audit feedback addressed	March 2027

Approval and Sign-Off

Role	Name	Signature	Date
Chief Executive	Dr Mudassir Tanveer		20/04/2026
Principal	Chris McLean		20/04/2026
Data Protection Officer (DPO)	Marlon Mason		20/04/2026
Governance Board Representative	Paul Jones		20/04/2026

Contacts

For queries regarding this policy or data protection matters:

- **Data Protection Officer (DPO):** Marlon Mason
- **Operational Contact:** Beverley Ball