



CASPIAN
SCHOOL OF ACADEMICS

Procedure 9.1

DATA PROTECTION

Data Governance and Management | August 2026



www.caspianschool.ac.uk

Data Protection

Data Governance and Management

Document Control

Document title	Data Protection
Document reference	Procedure 9.1
Policy category	Data Governance and Management
Document type	Procedure
Status	Current
Policy owner	Chief Executive Officer
Approved by	Board of Governance
Publication classification	Public
Current controlled version	Caspian Policy Library - caspianschool.ac.uk/policies/

Version History

Version	Approved by	Approval date	Effective date	Next review date
1.0	Board of Governance	14 August 2026	14 August 2026	14 August 2027

Table of Contents

INTRODUCTION.....	4
PRINCIPLES.....	4
RESPONSIBILITIES.....	4
Board of Governance.....	4
Senior staff.....	4
All staff.....	4
All students.....	5
COMPLIANCE.....	5
DATA PROTECTION COMPLAINTS.....	5
REVIEW.....	5
Data Protection Procedure.....	5
2. RESPONSIBILITIES OF STAFF.....	5
3. RIGHTS TO ACCESS INFORMATION.....	6
4. SUBJECT CONSENT.....	7
5. THE DATA CONTROLLER AND DATA PROTECTION LEAD.....	7
6. RETENTION OF DATA.....	7
7. CONCLUSION.....	7
Appendix 1.....	7
GUIDELINES FOR RETENTION OF PERSONAL DATA.....	7
Appendix 2.....	8
STANDARD REQUEST FORM FOR ACCESS TO DATA.....	8

INTRODUCTION

The School is committed to protecting the privacy of its students, staff and other individuals and to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025. Personal data must be processed lawfully, fairly and transparently, kept secure and disclosed only where there is an appropriate lawful basis.

Information that is already publicly available is not automatically outside data protection law. Where information identifies an individual, the School will continue to handle it in accordance with applicable data protection legislation. Subject to legal, regulatory and privacy requirements, the following institutional information may be made publicly available:

- names of our Directors
- names of independent external Board of Governance members
- names of staff members

PRINCIPLES

The School, its staff and others who process personal data must follow the data protection principles in the UK GDPR and the requirements of the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. The School is registered with the Information Commissioner's Office and will ensure that personal data is processed in accordance with the following requirements:

- obtained and processed fairly and lawfully
- obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose
- adequate, relevant and not excessive for those purposes
- accurate and kept up to date
- not kept longer than is necessary for that purpose
- processed in accordance with the data subject's rights
- kept safe from unauthorised access, accidental loss or destruction
- not transferred outside the UK unless the transfer is permitted under applicable data protection law, for example through adequacy regulations, appropriate safeguards or another lawful transfer mechanism

The School will disclose staff or student personal data to third parties only where there is an appropriate lawful basis and the disclosure complies with applicable data protection requirements. Consent will be sought where consent is the appropriate lawful basis.

RESPONSIBILITIES

Board of Governance

The Board of Governance is responsible for the oversight and implementation of this procedure

Senior staff

Senior staff are responsible for ensuring compliance with this procedure and communicating its requirements to all staff.

All staff

All members of staff are responsible for ensuring that personal data they hold is kept securely and is not disclosed to any unauthorised third party. All staff are also responsible for ensuring that personal data they provide to the School is accurate and up to date.

All students

All students are responsible for ensuring that all personal data provided to the School is accurate and up to date.

COMPLIANCE

Failure to comply with the data protection procedure could result in disciplinary action.

DATA PROTECTION COMPLAINTS

The School will provide a clear route for individuals to make a data protection complaint. Complaints will be acknowledged within 30 days of receipt. The School will investigate the matter, keep the complainant appropriately informed and communicate the outcome without undue delay. Individuals will also be informed of their right to complain to the Information Commissioner's Office where appropriate.

REVIEW

This procedure will be reviewed on an annual basis

Data Protection Procedure

The School needs to process certain information about its employees, students and other users for purposes including recruitment, attendance, performance, achievement, health and safety, payroll, course administration and compliance with legal or regulatory obligations. Personal data must be processed lawfully, fairly and transparently, kept secure and not disclosed unlawfully. The School will comply with the data protection principles set out in the UK GDPR and related UK data protection legislation.

The School and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed the Data Protection Procedure, available on the Staff Net.

The School requires a confidentiality statement to be signed by all those who have access to student and staff data.

2. RESPONSIBILITIES OF STAFF

2.1 Information about yourself

All staff share responsibility for:

- checking that any information they provide to the School in connection with their employment is accurate and up-to-date
- informing the School of any changes to information, which they have provided, i.e. change of address
- informing the School of any errors or changes. The School cannot be held responsible for any errors unless the staff member has informed us of them

2.2 Information about students

This applies to all staff who process and access data about individuals on a regular basis, i.e. when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. The information must be provided to only relevant parties deemed fit by the School.

The School will ensure that each processing activity has an appropriate lawful basis and that individuals are provided with relevant privacy information. The information staff handle on a day-to-day basis will commonly include categories such as:

- general personal details, such as name and address

- details about class attendance, course work marks and grades and associated comments
- notes of personal supervision, including matters about behaviour and discipline

Information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, health, sex life or sexual orientation is special category personal data. It may be processed only where an appropriate Article 6 lawful basis and Article 9 condition apply, together with any additional condition required by the Data Protection Act 2018.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in this procedure. In particular, staff must ensure that records are:

- accurate
- up-to-date
- fair
- kept and disposed of safely and responsibly

The Principal is responsible for ensuring that appropriate organisational arrangements are in place to keep personal data secure. In particular, personal data must be:

- put away in lockable storage
- not left on unattended desks or tables
- not be accessible to other users
- ICT equipment used off-site must be password-protected
- personal data stored on removable media or sent in email attachments for authorised off-site use must be appropriately protected, including by encryption or password protection where required
- paper records containing personal data must be shredded where appropriate

Staff shall not disclose personal data to any other staff member, except with the authorisation or agreement of the designated data controller, or in line with School procedures.

Before processing any personal data, all staff should consider the following.

- Do you really need to record the information?
- Is the information 'sensitive'?
- If it is special category data, have you identified the relevant Article 9 condition and any additional Data Protection Act 2018 condition?
- Has the individual been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If consent is not the lawful basis, have you identified and documented another appropriate lawful basis and, where applicable, a special category condition?
- *Administration staff should take particular care to ensure that private or confidential information is disclosed only to the intended recipient. For example, emails and documents circulated to students requiring student signature should not contain sensitive information such as date of birth and that student emails will not be disclosed to other students. Staff will use the BCC facility when sending block emails to learners.*

3. RIGHTS TO ACCESS INFORMATION

Staff, students and other individuals have the right to request access to personal data the School holds about them. A person wishing to exercise this right may use the School Standard Request Form for Access to Data (Appendix 2) or make a valid request by another recognised method. Requests should be directed to the Principal or the School's designated data protection contact.

The School will normally respond to a subject access request without charge. A reasonable fee may be charged only where permitted by law, including where a request is manifestly unfounded or excessive or where further copies are requested.

The School will respond to a subject access request without undue delay and normally within one month of receipt. Where the law permits an extension because a request is complex or numerous, the individual will be informed within one month and given the reason for the extension.

4. SUBJECT CONSENT

The School will identify and document an appropriate lawful basis for each processing activity. Consent will be used only where it is appropriate and valid. Additional legal conditions apply to special category data and criminal offence data.

The School also has a duty of care to all staff and students and must therefore make sure those employees and those who use the School facilities do not pose a threat or danger to other users.

The School may request information about health needs where this is necessary to support an individual, protect health and safety or meet legal obligations. Health information will be processed only where an appropriate lawful basis and special category condition apply, including where processing is necessary to protect vital interests or meet relevant legal obligations.

Prospective staff and students will be given appropriate privacy information explaining why personal data is required and the lawful basis for processing it. Where information is genuinely necessary for legal, contractual, safeguarding or enrolment purposes, failure to provide it may affect the School's ability to proceed with employment or enrolment.

5. THE DATA CONTROLLER AND DATA PROTECTION LEAD

The School is the data controller for personal data where it determines the purposes and means of processing. The Board of Governance has oversight of implementation, with day-to-day responsibilities delegated through the School's management arrangements.

The Principal is the designated senior lead for day-to-day data protection matters and will ensure that queries, rights requests and complaints are directed to the appropriate person for action.

6. RETENTION OF DATA

Please see Appendix 1 for the guidelines for the retention of personal data.

7. CONCLUSION

Compliance with applicable data protection legislation is the responsibility of all members of the School. A breach of this procedure may result in disciplinary action, withdrawal of access to School systems or facilities, and, where relevant, regulatory or criminal consequences. Questions or concerns about this procedure should be referred to a line manager, the Principal or the School's designated data protection contact.

Appendix 1

GUIDELINES FOR RETENTION OF PERSONAL DATA

Type of data	Suggested retention period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation
Application forms/interview notes	At least 6 months from the date of the interviews.	Time limits on litigation

Type of data	Suggested retention period	Reason
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies	Limitation Act 1980
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As Above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As Above	Statutory Sick Pay (General) Regulations 1982
Wages and Salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 2013
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness.	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1994	40 years	COSHH 2002
Student records, including academic achievements, and conduct	At least 6 years from the date the student leaves the School, in case of litigation for negligence, At least 10 years for personal and academic references, with the agreement of the student	Limitation period for negligence

Appendix 2

STANDARD REQUEST FORM FOR ACCESS TO DATA

I.....wish to have access to either:

1. All the data that Caspian School of Academics (CSA) currently has about me, either as part of an electronic system or part of a relevant filing system; or
2. Data that Caspian School of Academics (CSA) has about me in the following categories:
 - Academic marks or course work details
 - Academic or employment references
 - Disciplinary records
 - Health and medical matters
 - Any statements of opinion about my abilities or performance
 - Personal details including name, address, date of birth etc
 - Other information

(Please tick as appropriate)

I understand that subject access requests are normally handled free of charge, subject to the limited circumstances in which a reasonable fee is permitted by law.

Signed

Dated: