



CASPIAN
SCHOOL OF ACADEMICS

Policy 9.0

DATA GOVERNANCE AND MANAGEMENT POLICY

Data Governance and Management | August 2026



www.caspianschool.ac.uk

Data Governance and Management Policy

Data Governance and Management

Document Control

Document title	Data Governance and Management Policy
Document reference	Policy 9.0
Policy category	Data Governance and Management
Document type	Policy
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
1.1	Board of Governance	14 August 2026	14 August 2026	14 August 2027

Table of Contents

Introduction.....	4
Scope.....	4
Data Access.....	4
Data Management Standards.....	4
Information Controller / owner.....	5
Data Experts.....	5
Data Users.....	5
Data.....	5
Data Management Framework.....	6
Data Owner.....	6
Chief Executive Officer.....	6
Information Owners.....	7
Data Experts.....	7
Data Users.....	7
Data users must:.....	8
Unstructured Data.....	8
Associated procedures.....	8

Introduction

Caspian School of Academics has a clear responsibility to manage and maintain the integrity, legality and security of the information it gathers and manages. The Data Governance and Management Policy sets out the key responsibilities and criteria for Data Management.

Scope

The Caspian School of Academics (CSA) has developed a Data Governance and Management Policy which applies to:

- data, in all its forms - structured or unstructured, which is required for the management and administration of the School and the conduct of its work, whether the data sets are captured and accessed from on-campus or off-campus locations;
- all CSA activities;
- individual Members of the School within their designated roles (Admissions, Teaching, Quality Monitoring, Data Management, Funding);
- the School's awarding bodies to whom data must be submitted according to awarding body stipulated requirements.
- collaborative activities undertaken with partner organisations, as appropriate.

All data created or owned by CSA are the property of the School and are regarded as corporate assets.

The data created or owned by the School shall include, but not be limited to, data relating to management and administration and to the conduct of the School's business.

The School recognises the value of data as an institutional resource and considers that value to be increased through the widespread and appropriate use of data and by virtue of data quality.

CSA considers the value of data to be diminished through misuse, misinterpretation or unnecessary access restrictions.

Data Access.

Access to data will be granted to Data Users for legitimate purposes related to the work of the School and in accordance with applicable data protection law, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. Access is also subject to approved role-based restrictions and other legal, regulatory and information-security requirements.

Data access is determined on behalf of the School by the Chief Executive Officer. CSA is committed to the Data Management Standards set out in this document.

Data Management Standards

The School categorises and determines data access as follows:

Internal. Data categorised as 'Internal' may be accessed by all Data Users, which includes academic and support staff for records and report purposes.

Confidential or Highly Confidential. At the discretion of the School, specific data may be categorised as 'Confidential' or 'Highly Confidential'. Data will be categorised as 'Confidential' or 'Highly Confidential' by the Chief Executive Officer in accordance with applicable data protection law, information-security requirements, notification from the data owner and, where appropriate, legal or other regulatory advice.

Public. Data that the School determines may lawfully and appropriately be made freely available without restriction are categorised as 'Public'.

Data will be categorised as 'Public' by the Chief Information Officer in the light of recommendations from data source/owner, Freedom of Information requirements and, where appropriate, legal and other regulatory advice.

Information Controller / owner

Every data source and Dataset must have a designated Information Controller or Owner.

Information Ownership of a Dataset will be delegated to the Chief Executive Officer or the Head of Data Management or other manager with primary responsibility for the School's operations to which the Dataset relates.

The Information Controller / Owner is responsible for the data quality, security and availability of the data they manage.

Data Experts

Data Experts are responsible for and accountable to the relevant Information Owners, including for:

- a. the operational management of the assigned institutional data and its integrity;
- b. applying the School's data management standards and procedures;
- c. effective liaison with the technical experts responsible for the repositories where the data are stored and for the applications and reporting systems for use of the data;
- d. data analysis;
- e. providing management information to support CSA decision-making;
- f. external reporting requirements;
- g. resolving queries;
- h. implementing agreed data retention criteria and archiving policies;
- i. making the Data Dictionary understandable to users.

Data Users

Subject to any data access restrictions determined on behalf of the School by the Chief Executive Officer (CEO), permission to access data will be granted to:

- all staff for legitimate CSA purposes and
- other individuals, where agreed, following the data access approval by the CEO.

Data Users are required to:

- i. access and use data only in their conduct of CSA business;
- ii. access only the data needed to carry out their CSA work;
- iii. respect the confidentiality and privacy of individuals whose records they may access;
- iv. observe any ethical, commercial, security or other restrictions determined by the School that apply to the data to which they have access;
- v. comply with all relevant legal requirements;
- vi. comply with the Data Management Standards;
- vii. work within the limits of the data access that they have been granted.

Data

Data management:

1. must be readily available to all Data Users with a legitimate CSA business need through easily accessible web-based interfaces;
2. must be stored in an official School data repository agreed with the CEO (or nominee);

3. should be defined consistently across the School;
4. element names, formats and codes must be consistent across all repositories and information systems that use the data and consistent with agreed standards;
5. should, wherever possible, be captured or entered once only;
6. structures must be under strict change control so that business and system implications of any change can be properly managed;
7. for data capture, validation and processing should, wherever possible, be automated;
8. updating processes should be standard across the School and its systems;
9. should be recorded in an auditable and traceable manner and in accordance with any agreed change control processes;
10. should not be duplicated unless duplication is absolutely essential and has the approval of the relevant Information Owner; in such cases, one source must be clearly identified as the master and there must be a robust process to ensure copies are not modified and are kept in step with the master source;
11. exchange protocols between data repositories must be under strict change control so that business and system implications of any change can be properly managed.

Arrangements for the storage and use of all data, including any third-party use, must conform with Procedure 9.1 - Data Protection.

Whenever possible, international, national or industry standards for common data models must be adopted. When this is not possible, institutional standards will be determined.

Data Management Framework

The following structure forms an institutional Data Management Framework, the purpose of which is to ensure data are consistent, of good quality and available for use by Data Users.

Data Management Framework

Data Owner

The School is the data controller for personal data where it determines the purposes and means of processing. "Data Owner" in this policy is an internal governance role and does not replace the legal concept of controller under data protection law.

Chief Executive Officer

The Chief Executive Officer, advised and assisted by the Data Manager and staff responsible for programme information management (programme administration) is responsible for:

1. for data management policy, standards and procedures;
2. for the School's data model, its promotion and its implementation;
3. for monitoring and reviewing the effectiveness of data management policy, standards and procedures;
4. formulating data management policy and standards for approval by the Board of Governance;
5. advising the Board on their implementation;
6. establishing procedures for the management of and access to data;
7. overseeing the implementation of and compliance with data management policy, standards and procedures;
8. adjudicating on any disputes that may arise from time to time;
9. in conjunction with Information Owners, reviewing annually, the Data Governance and Management Policy

Information Owners

Information Owners are responsible for and accountable to the CEO for:

1. the management of the assigned institutional data;
2. co-ordination of the associated Data Experts;
3. the collection and updating of the assigned institutional data;
4. recommending changes to institutional data management policy and procedures;
5. data quality;
6. the implementation of Data Management Standards and procedures;
7. the promotion of the management of School data as a vital institutional resource;
8. understanding and promotion of the value of data for CSA-wide purposes and facilitation of data sharing and integration;
9. authorisation and management of any third party use of the data in accordance with CSA policies and processes;
10. liaison with other Information Asset Owners as required;
11. advising and reporting on data management issues to the CEO.

Data Experts

Data Experts are responsible for and accountable to the relevant Information Owner for:

1. the operational management of the data assigned to them and its integrity;
2. applying CSA data management standards and procedures;
3. effective liaison with the technical experts responsible for the repositories where the data sets are stored and for the applications and reporting systems for use of the data;
4. data analysis;
5. providing management information to support CSA decision-making;
6. external reporting requirements;
7. resolving queries;
8. implementation of agreed data retention criteria and archiving policies;
9. making the Data Dictionary understandable to users.

Data Users

Data Users are responsible for and accountable to their managers for:

1. ensuring their use of the data complies with this policy and all related standards and procedures;
2. for all data access made through their user account and the subsequent use and distribution of the data;
3. identifying any potential personal conflicts of interest resulting from the authorised data access granted to them through their user account (including potential conflicts of interest where the data user is both a member of staff and student of the School) and for seeking advice from the relevant Information Owner;
4. for obtaining permission from the Information Owner for use of the data for marketing campaigns or other contact list purposes;
5. for contributing to the accuracy and integrity of the data through the timely correction and updating of data where authorised to do so and for other data, through timely notification to the relevant Information Owner.

Data users must:

- a. not disclose their user login account password to anyone;
- b. not use data for their own personal gain or for the gain or profit of others;
- c. not access data for personal business purposes or personal interest;
- d. not disclose data to unauthorised persons or to any third party without the consent of the relevant Information Owner;
- e. not disclose data about an individual to another person, regardless of that person's relationship with the individual concerned, without the consent of the individual concerned and/or without the consent of the relevant Information Owner;
- f. present the data accurately and objectively in any use that is made of it.

Unstructured Data

Whilst structured data is usually held within a controlled environment on the School's servers, unstructured data (in the form of files and documents) are usually under the control of the user/data processor who created them, and stored in file storage where access cannot be so easily centrally regulated. For this reason it is essential that the owners of those documents take responsibility for their security, dependent on the type of data which is contained within.

The School provides advice and guidance on where documents should be stored and how they should be protected. This guidance (which may change from time to time) must be followed in order to protect CSA data and personal and confidential data from accidental or deliberate leakage. In particular, data classified as 'Confidential' or 'Highly Confidential' must be protected accordingly.

Associated procedures

- Procedure 9.1 Data Protection
- Procedure 9.2 Oversight of Information and Data Returns
- Procedure 9.3 Appropriate Use of Information Technology