Cardiff Academy

POLICY /// INFORMATION AND DATA

Data Protection and Records Management Policy

How Cardiff Academy collects, uses, shares, protects and retains personal data about students, applicants, parents, staff and others in line with UK GDPR, including data sharing with universities, agents and UKVI, CCTV, individual rights, data breaches and the records retention schedule.

REFERENCE	**CA-INF-01**	VERSION	**1.0 (Approved)**
POLICY OWNER	**Data Protection Lead**	APPROVED BY	**Board of Governors**
ISSUE DATE	**October 2026**	APPROVAL DATE	**October 2026**
REVIEW CYCLE	**Annual**	NEXT REVIEW DUE	**October 2027**
APPLIES TO	**All staff, governors, contractors and agents with access to personal data**	PUBLISHED	**Website (summary and privacy notices); staff portal**

RELATED POLICIES CA-INF-02 Privacy Notice for Students and Applicants; CA-INF-03 Online Safety, Acceptable Use, Social Media and Images; CA-ADM-03 UKVI Sponsor Compliance; CA-WEL-01 Safeguarding and Child Protection; CA-GOV-04 Business Continuity

LEGAL ENTITY Cardiff Education Group Ltd, trading as Cardiff Academy (Company No. 14569122). Registered office: 168 City Road, Cardiff CF24 3JE. Teaching premises: 8 Drake Walk, Cardiff CF10 4LG

1 Policy statement

Cardiff Academy respects the privacy of everyone whose personal data it holds. We will process personal data lawfully, fairly and transparently, keep it secure, and use it only for the purposes for which it was collected. Cardiff Education Group Ltd is the **data controller** and is registered with the Information Commissioner's Office.

2 Scope

This policy applies to all personal data processed by the Academy in any format (electronic, paper, audio, video, CCTV), about applicants, students, former students, parents and guardians, sponsors, staff, job applicants, governors, agents, visitors and contractors.

3 Data protection principles

Personal data must be:

1. processed lawfully, fairly and transparently
2. collected for specified, explicit and legitimate purposes
3. adequate, relevant and limited to what is necessary
4. accurate and kept up to date
5. kept for no longer than necessary
6. processed securely

The Academy must be able to **demonstrate** compliance (accountability).

4 Roles

Role	Responsibility
Board of Governors	Overall accountability; receives an annual data protection report
Data Protection Lead (Sajid Hussain)	Day-to-day compliance; advice; Record of Processing Activities (ROPA); data protection impact assessments (DPIAs); responding to rights requests and breaches; training. The Academy is not required to appoint a statutory Data Protection Officer, but has designated this role
Senior managers	Ensure systems and processes in their areas comply
All staff	Follow this policy; complete training; report breaches immediately

5 Lawful bases

Purpose	Main lawful basis
Processing applications, enrolment, teaching, assessment and certification	Contract
UKVI sponsor duties (passport and visa copies, attendance, reporting)	Legal obligation
Safeguarding and welfare, including sharing with social services and police	Legal obligation; vital interests; public task / substantial public interest (safeguarding of children and individuals at risk)
Health and disability information to provide support and adjustments	Explicit consent, or substantial public interest / vital interests where appropriate
Sharing results and progression data with partner universities	Contract (with the student) and legitimate interests; explained in the privacy notice
Marketing to applicants and alumni	Consent (electronic marketing) or legitimate interests

Purpose	Main lawful basis
Photographs and video for publicity	Consent
CCTV for safety and security	Legitimate interests
Staff employment records, payroll, right-to-work and DBS checks	Contract; legal obligation

Special category data (health, ethnicity, religion, sexual orientation, biometric data) and criminal offence data are processed only where an Article 9 condition and, where needed, a Schedule 1 DPA 2018 condition apply, as recorded in the Academy's **Appropriate Policy Document**.

6 Privacy notices

The Academy provides privacy notices to applicants and students (CA-INF-02), staff and job applicants, parents, and website users, explaining what data we hold, why, who we share it with, how long we keep it, and individuals' rights.

7 Sharing data

We share personal data only where there is a lawful basis and it is necessary. Regular sharing is governed by written agreements:

Recipient	Purpose	Agreement
Partner universities	Applications for progression, confirmation of results and attendance, transfer of student records	Data sharing schedule within each partnership agreement
UK Visas and Immigration	Sponsor reporting and compliance	Statutory obligation
Education agents	Processing applications	Data protection schedule in the Agent Agreement
Sponsors (governments, employers)	Attendance and progress reports	Student consent or sponsor agreement disclosed at enrolment
Awarding and examination bodies	Registration and results	Awarding body terms
Local authority, police, health services	Safeguarding, prevention or detection of crime, emergencies	Lawful basis assessed case by case; recorded by the DSL
Processors (MIS, email, cloud storage, payroll, IT support)	Providing services to the Academy	Article 28 processor contracts

Personal data is transferred outside the UK only where appropriate safeguards are in place (UK adequacy regulations, the International Data Transfer Agreement or Addendum, or an Article 49 derogation such as performance of a contract with the student).

8 Individuals' rights

Individuals have the right to be informed, to access their data, to rectification, to erasure, to restrict processing, to data portability, to object, and rights in relation to automated decision-making.

- Requests may be made verbally or in writing to enquiries@cardiffacademy.co.uk or any member of staff, who must pass them to the Data Protection Lead the same day.
- We will verify the requester's identity and respond **within one month**, which may be extended by up to two further months for complex requests. Searches will be reasonable and proportionate.
- Requests made on behalf of a student (for example by a parent or agent) require the student's consent where the student is aged 13 or over and able to understand their rights, unless the law provides otherwise.
- Exam scripts are exempt from access, but marks and examiners' comments are not.

9 Data protection complaints

Anyone who is unhappy with how we have handled their personal data may complain to the Data Protection Lead. We will acknowledge the complaint within **30 days**, investigate it without undue delay, and tell the complainant the outcome, as required by the Data (Use and Access) Act 2025. Complainants may then contact the ICO.

10 Security

- Access to personal data is restricted by role. Accounts are individual and protected by strong passwords and multi-factor authentication.
- Laptops and mobile devices are encrypted. Personal data is not stored on personal devices or removable media unless encrypted and authorised.
- Paper records are kept in locked cabinets; confidential waste is shredded.
- Safeguarding records are kept separately from the main student file, with access limited to the DSL team.
- Data is backed up and recovery is tested (CA-GOV-04).
- Staff complete data protection and cyber security training at induction and annually.

11 Data protection by design and DPIAs

A data protection impact assessment is completed before any new system, process or data sharing arrangement that is likely to present a high risk (for example new student records software, biometric attendance systems, CCTV changes, AI tools that process student data).

12 Personal data breaches

1. Any member of staff who becomes aware of a breach (loss, theft, unauthorised access, accidental disclosure, ransomware) must report it immediately to the Data Protection Lead.
2. The Data Protection Lead contains the breach, assesses the risk and records it in the **Breach Log**.
3. Where the breach is likely to result in a risk to individuals' rights and freedoms, it is reported to the **ICO within 72 hours** of the Academy becoming aware.
4. Where there is a high risk, affected individuals are told without undue delay.
5. Partner universities, UKVI or sponsors are notified where agreements require.

13 CCTV and attendance technology

- CCTV operates at the entrances and communal areas of the premises for safety, security and the prevention of crime. It is not used in toilets or changing areas, or to monitor teaching performance.
- Signs inform people that CCTV is in operation and who to contact.
- Footage is retained for **30 days** unless required for an investigation, and is accessed only by authorised staff.
- Requests for footage are handled as subject access requests or under the relevant legal exemption.
- Any biometric attendance or access system (for example fingerprint or facial recognition) is used only after a DPIA, with explicit consent and an alternative available for anyone who does not consent.

14 Artificial intelligence tools

Staff must not enter personal data about students, staff or applicants into public generative AI tools. Approved AI tools are listed by the Data Protection Lead following a DPIA.

15 Records retention schedule

Records are kept for the periods below and then securely destroyed, unless a legal hold applies.

Record	Retention period	Owner
Unsuccessful applications	1 year from decision	Admissions
Student file (application, enrolment, contact, correspondence)	6 years after the student leaves	Admissions and Compliance
UKVI sponsored student records (passport, visa, CAS, attendance, contact details, qualifications used for CAS)	Duration of sponsorship plus at least 1 year, or until a compliance officer has examined and approved them, whichever is later; the Academy keeps them for 6 years	Admissions and Compliance
Attendance registers	6 years after the student leaves	Academic administration
Assessment scripts and coursework	1 year after the Assessment Board, or until any appeal is concluded	Director of Studies
Marks, Assessment Board minutes, transcripts and award records	Permanently (to verify awards)	Principal
Safeguarding and child protection records	Until the student's 25th birthday, or 6 years after leaving if later; longer where there are allegations against staff (retained until normal retirement age or 10 years, whichever is longer); records relevant to any inquiry are kept until it concludes	DSL
Complaints and appeals	6 years from closure	Complaints Coordinator

Record	Retention period	Owner
Accident and incident records	3 years (adults); until age 21 for students injured under 18; longer for RIDDOR or claims	Head of Operations
Staff personnel files	6 years after employment ends	HR
Staff right-to-work evidence	Employment plus 2 years	HR
DBS certificate information	Record of check (date, number, outcome) on the Single Central Record; certificate copies not retained beyond 6 months	HR
Recruitment records for unsuccessful candidates	6 months	HR
Financial records	6 years from the end of the financial year	CFO
CCTV footage	30 days	Head of Operations
Marketing consent records	Until consent is withdrawn plus 2 years	Marketing

16 Monitoring and review

The Data Protection Lead reviews the ROPA, privacy notices and this policy annually, audits compliance in a sample of areas each year, and reports to the Board.

Compliance mapping

This policy has been written to meet, and to evidence, the following external requirements. Inspectors and university partners can use this table to locate the relevant provisions.

ISI Educational Oversight (PFE) standards	Standard 33 (accurate admission and attendance registers); Standard 64 (records of staff checks); Standard 63 (prompt responses to requests for information)
British Council Accreditation UK criteria	M16–M17 (accurate enrolment, payment and contact records); M8 (HR policies)
UKVI Student sponsor guidance	Student sponsor guidance – record-keeping duties (Appendix D), retention for the required period and availability to compliance officers
University partner due diligence	Partner due diligence – data protection policy; data sharing agreements for applications, progression and student records
Legislation and statutory guidance	UK General Data Protection Regulation; Data Protection Act 2018; Data (Use and Access) Act 2025; Privacy and Electronic Communications Regulations 2003; Freedom of Information does not apply to the Academy; ICO CCTV and surveillance guidance; Keeping Learners Safe (Wales, 2022) on safeguarding records

Document control

Version	Date	Author / reviewer	Summary of changes

0.9	Pre-2026	Various	CA DATA PROTECTION POLICY; CA GDPR Privacy Policy (2025); CA Data Protection Policy (JCQ, 2025); CCTV policy
1.0	October 2026	Data Protection Lead	New policy written for university partnerships, ISI Educational Oversight and British Council Accreditation UK. Supersedes all previous versions.

APPROVED ON BEHALF OF THE BOARD	SIGNATURE	DATE
Chair of the Board of Governors		