Data Protection Policy

Document Code	TA-DPR-04: Data Protection Policy
Principal Contact	
Date Effective from	03.08.2025
Review Date	Every 3 years or earlier when required
Version	V1.0 2025
External Reference Points	• Data Protection Act 2018 • UK GDPR (incorporating EU GDPR provisions) • Information Commissioner's Office (ICO) guidance • GDPR 7 Principles: Lawfulness, fairness, transparency; Purpose limitation; Data minimisation; Accuracy; Storage limitation; Integrity and confidentiality; Accountability. • OfS Condition F1: Accurate information provision. • UK Quality Code 2024 Principle 4: Adhering to ethical and data protection requirements in data use. • Consumer Rights Act 2015 for transparency in data notices; AI Act (draft) for emerging tech compliance; Freedom of Information Act 2000 for public sector duties.

Summary/Description

This policy ensures compliance with data laws for personal information handling by the academy, covering all staff, students, affiliates, and third parties across all activities, including online platforms, international data transfers, research projects, and AI-driven data processing. It applies to all forms of personal data, whether electronic or paper-based, processed for academy purposes, and extends to data held on academy systems, personal devices used for work, or by external processors. The policy now incorporates data protection by design and default principles, special considerations for research data, and provisions for anonymisation and pseudonymisation to minimise risks.

Contents

1. Policy Statement

1.1 Trafalgar Academy is committed to protecting the privacy, confidentiality, and security of personal data in compliance with the UK GDPR, Data Protection Act 2018, and other relevant legislation. We recognise the importance of handling personal information responsibly, transparently, and ethically to build trust with our students, staff, partners, and stakeholders. This policy affirms our dedication to upholding data subject rights, implementing robust safeguards against risks, and fostering a culture of data protection awareness across all academy activities. By adhering to the seven GDPR principles, we ensure that personal data is processed lawfully, fairly, and securely, with accountability at every level.

2. Aims and Objectives

2.1 To protect data rights, minimise risks, and build trust with stakeholders. Objectives include secure, lawful, and transparent processing; mandatory staff and student training; effective risk management through assessments; accountability via record-keeping; promoting data literacy; and ensuring compliance with data subject rights to foster a culture of privacy respect.

3. Principles

- **3.1 Fairness** is central to the admissions process, meaning all decisions are made without discrimination and incorporate positive action measures where appropriate to level the playing field for applicants from diverse backgrounds.
- **3.2 Transparency** ensures that criteria, processes, and timelines are clearly published and communicated, allowing applicants to understand expectations and prepare accordingly.
- **3.3 Inclusivity** guides the policy by promoting contextual admissions that address barriers such as socioeconomic disadvantages, and by providing accommodations for applicants with disabilities to ensure equal access.
- **3.4 Integrity** requires that all information provided by applicants is accurate and verifiable, with robust checks in place to maintain trust in the system.
- **3.5 consumer-focused** approach aligns the policy with terms and conditions that protect applicant rights, emphasising clear information on offers, fees, and withdrawal options to comply with legal standards.

4. Definitions

- **4.1 Personal Data:** Information identifying individuals, e.g., names, emails, biometric data, or opinions about them.
- **4.2 Special Category Data:** Sensitive data like health, ethnicity, racial origin, political opinions, religious beliefs, trade union membership, sexual orientation, genetic data, or criminal convictions, requiring extra safeguards and explicit conditions for processing.
- **4.3 Data Breach:** Unauthorised access, loss, disclosure, alteration, or destruction of data.
- **4.4 Data Subject Rights:** Rights to access, rectify, erase, restrict, object to, or port data, and rights related to automated decision-making.
- **4.5 Data Subject:** A living individual to whom personal data relates.
- **4.6 Data Controller:** The academy, determining the purposes and means of processing.
- **4.7 Data Processor:** Third parties processing data on the academy's behalf, e.g., cloud service providers.
- **4.8 Third Party:** Any entity other than the data subject, controller, or processor.
- **4.9 Anonymisation:** Rendering data non-identifiable irreversibly.

- **4.10 Pseudonymisation:** Replacing identifiers to prevent direct identification without additional information.

5. Procedures

5.1 Processing: Identify and document lawful bases (e.g., consent, contract, legal obligation, legitimate interests) for all activities; conduct mandatory Data Protection Impact Assessments (DPIAs) for high-risk processing, such as new AI systems or large-scale data collection, using a standardised template to identify risks and mitigations. Consent must be freely given, specific, informed, and easily withdrawable via email, portal, or dedicated form, with records maintained. Privacy notices must be provided at the point of data collection, detailing purposes, retention periods, rights, and sharing details.

5.2 Security: Implement technical and organisational measures including encryption for sensitive data, two-factor authentication, access controls (role-based), regular security audits, and secure disposal methods (e.g., shredding paper, certified data wiping for devices). For mobile devices and remote working, require password protection and encryption; prohibit use of unapproved cloud services. Data sharing with third parties requires written agreements with security clauses and due diligence checks.

5.3 Breaches: Activate an incident response plan upon detection; assess risk and report to ICO within 72 hours if high risk to rights and freedoms; notify affected data subjects without undue delay if high risk, providing details on impacts and mitigation advice. Conduct root cause analysis and implement corrective actions, logging all incidents. Rights: Handle data subject requests (e.g., subject access requests for copies of data, rectification for inaccuracies, erasure under 'right to be forgotten', restriction of processing, objection to marketing, data portability) within one month, extendable by two months for complex cases; verify requester identity; provide responses in accessible formats. Appeals against decisions via the Complaints and Appeals Policy. International Transfers: Ensure adequate safeguards such as UK adequacy decisions, standard contractual clauses, binding corporate rules, or explicit consent; conduct transfer risk assessments for non-adequate countries.

5.4 Retention and Disposal: Retain data only as long as necessary per defined schedules (e.g., student records for 6 years post-graduation); review annually; securely dispose or anonymise when no longer needed.

5.5 Research Data: For research involving personal data, obtain ethics approval, minimise data use, anonymise or pseudonymise where possible, and inform participants via privacy notices; students processing data for studies must seek supervisor approval and comply with consent requirements.

5.6 Training: Mandatory annual data protection training for all staff and relevant students, covering principles, breaches, and rights; tracked via HR systems. DPIA Template: Includes risk scoring, stakeholder consultation, and DPO sign-off. Anonymisation Guidance: Techniques like aggregation or removal of identifiers.

5.7 Example 1: A student data breach (e.g., hacked database) triggers ICO notification, individual alerts, and system upgrades; a rights request for exam data access is fulfilled with redacted information within 30 days.

5.8 Example 2: AI tool processing student essays requires DPIA to assess privacy risks and pseudonymisation of inputs; international data transfer to a US partner uses standard clauses with risk assessment.

6. Responsibilities

- **6.1 Data Protection Officer (DPO):** Oversee compliance, advise on DPIAs and high-risk processing, handle complaints and ICO liaison, conduct audits, and provide training.
- **6.2 Staff:** Follow procedures, report breaches immediately, complete training, ensure data accuracy, and process data only for authorised purposes; supervisors ensure team compliance.
- **6.3 Students:** Provide accurate data, update details promptly, and comply when processing data for studies (e.g., with consent); report concerns.
- **6.4 Leadership:** Allocate resources for compliance, integrate data protection into governance and risk management, appoint Data Protection Champions as local contacts, and ensure third-party contracts include data protection clauses.
- **6.5 Third Parties/Processors:** Adhere to academy instructions, implement security measures, and report breaches promptly.
- **6.6** All Users: Familiarise with privacy notices and avoid unauthorised disclosures;
- **6.7** Researchers: Ensure ethical processing and minimisation.

7. Monitoring and Review

7.1 Annual compliance audits by DPO, including penetration testing, data mapping exercises, and reviews of processing activities; policy reviewed every two years or following breaches, legislative changes, or ICO guidance. Metrics include breach numbers and response times, rights request handling times and volumes, training completion rates (target: 100%), DPIA completion rates, and audit findings with action plans (enhanced KPIs). Oversight by an Information Governance Committee, with annual reports to the Governing Body.

8.Related Documents

- Data Privacy Notice and Consent Policy
- IT Security Policy
- Breach Reporting Procedure
- Complaints and Appeals Policy
- AI Use in Assessments Guidance
- Research Ethics Policy
- Information Security Policy
- Data Retention Schedule