TITLE: Data Protection Policy	REF:GOV003	VERSION:7
APPROVAL BODY: ALET board	DATE: 15.10.26	REVIEW DATE: 14.10.27
LEAD PERSON: Data Protection Officer		
VERSION	REVIEWER/APPROVAL	REVIEW NOTES
1: 21.10.20	ALET Board	DPO contact details amended Appendix 1 added
7. 15.10.26	ALET Board	Annual Review

Data Protection Policy

1. Policy Statement

This policy sets out expectations regarding Data Protection at ALET.

ALET (the "Trust") is the statutory **Data Controller** for all academies and central operations within the Trust. We are committed to protecting the privacy and security of personal data in compliance with the **UK GDPR** and the **Data Protection Act 2018,** as interpreted and explained by the Information Commissioner's Office (ICO).

It also draws on sector guidance and relevant education law.

Key legislation and guidance includes:

- UK GDPR and Data Protection Act 2018 (including principles, individual rights, lawful bases, special category and criminal offence data, security, accountability).
- Protection of Freedoms Act 2012 (biometric information of children in schools and colleges).
- ICO guidance on CCTV and video surveillance, security and personal data breaches.
- Department for Education (DfE) statutory guidance: Keeping Children Safe in Education (current edition) and non-statutory guidance: Teaching online safety in schools.
- DfE guidance: Searching, screening and confiscation (for the examination of electronic devices).
- Other relevant law: Human Rights Act 1998, Equality Act 2010, Computer Misuse Act 1990, Freedom of Information Act 2000, Education Acts and relevant regulations.

This overarching policy applies to all Trust employees, local governors, trustees, volunteers, and third-party contractors. It covers all personal data processed centrally or locally by individual academies.

Trust Governance Structure & Accountability

Accountability within ALET is centralised:

- **The Trust Board:** Holds ultimate legal responsibility for data protection compliance across the entire MAT.
- **Headteachers and the Executive Team:** Ensures that standardised IT security, data handling policies and procedures, and staff training are implemented across all member academies.
- **Local Governing Committees (LGCs):** Monitor local compliance, escalate potential data breaches to the central team, and ensure local school staff adhere to this policy.

2. Definitions

Personal data: Any information relating to an identified or identifiable living individual (for example, name, identification numbers, location data, online identifiers, or factors specific to identity).

Special category personal data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data for identification, health data, or data concerning sex life or sexual orientation.

Processing: Any operation performed on personal data, whether automated or not (such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, erasure or destruction).

Data subject: The identified or identifiable individual whose personal data is processed.

Data controller: The organisation that determines the purposes and means of the processing of personal data (ALET).

Data processor: A person or organisation (other than the controller's employees) that processes personal data on behalf of the controller.

Personal data breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

ICT facilities: The school's ICT network, services, systems, hardware and software (including cloud services), whether used on-site or remotely, on school or authorised personal devices.

Users: Anyone authorised by the school to use the ICT facilities, including trustees, staff, students, volunteers, contractors and visitors.

Personal use: Any use not directly related to a user's employment, study or official purpose.

Authorised personnel: Employees or contractors authorised by the school to administer and/or monitor the ICT facilities.

Materials: Files and data created or stored using ICT facilities (documents, photos, audio, video, web pages, social networking, blogs, etc.).

3. The Data Protection Officer (DPO)

The Trust appoints a **centralised Data Protection Officer (DPO)** who oversees compliance across all academies.

Contact Details external DPO: Jules Carmichael **dposervicesltd@outlook.com**

For all Subject Access Requests (SARs), Freedom of Information (FOI) requests, and suspected data breaches, you must notify both: dpo@alet.org.uk and dposervicesltd@outlook.com

Using both email addresses ensures that the Internal Compliance Lead and External DPO are notified immediately and that statutory deadlines can be met.

Role: The DPO acts as the primary contact for the Information Commissioner's Office (ICO), conducts annual compliance audits at each academy, and advises trustees, headteachers, and local governors on complex data protection matters.

4. Cross-Academy Data Sharing

Personal data may be shared between member academies and the central Trust team when strictly necessary for legitimate operational or educational purposes:

- **Operational Efficiency:** Sharing HR, payroll, and central procurement data.
- **Educational Continuity:** Transferring pupil records seamlessly if a student moves between academies within the Trust.
- **Intervention:** Accessing pupil performance data by Trust directors to deploy targeted educational support.

All intra-Trust data sharing is governed by strict access controls. Staff only have access to records required to fulfil their specific role.

Data protection principles

The Trust adheres to the data protection principles set out in the UK GDPR. Personal data must be:

- Processed lawfully, fairly and transparently;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary; and

- Processed in a manner that ensures appropriate security (confidentiality, integrity and availability).
- Accountability: the school is responsible for, and must be able to demonstrate, compliance with these principles.

5. Lawful Bases for Processing

Before collecting or sharing any data, the Trust identifies the appropriate legal basis under Article 6 of the UK GDPR:

- **Public Task:** Delivering national curriculum education, tracking pupil progress, and maintaining student safeguarding.
- **Legal Obligation:** Complying with statutory Department for Education (DfE) census returns, tax regulations (HMRC), and child protection laws.
- **Consent:** Used for optional activities such as school marketing, promotional photos, or biometric dinner systems. Consent is managed locally by each academy but must be documented clearly and can be withdrawn at any time.

Collecting personal data

Lawfulness, fairness and transparency: We process personal data only where a lawful basis applies (contract, legal obligation, vital interests, public task, legitimate interests, or consent). For special category data we also meet a condition in Article 9 UK GDPR or the DPA 2018 (for example, employment law, vital interests, substantial public interest, health or social care, public health, or research). For criminal offence data we meet a lawful basis and an appropriate condition in the DPA 2018. We adapt consent collection based on the age/maturity of the pupils.

We provide data subjects with the information required by data protection law when we first collect personal data (via privacy notices) and we will not use personal data in ways that are unfair or unexpected.

Limitation, minimisation and accuracy: We collect personal data for specified, explicit and legitimate purposes, and will not use it for incompatible purposes without informing individuals and, where necessary, obtaining consent. Staff will only process the personal data they need to carry out their roles. We keep data accurate and up to date and rectify or erase inaccurate data when appropriate. When personal data is no longer needed, we delete or anonymise it in line with our retention schedule.

6. Technical & Centralised Security Measures

The Trust enforces standardised technical and organisational security requirements across all sites:

- **Centralised Identity Management:** Single Sign-On (SSO) and mandatory Multi-Factor Authentication (MFA) for all staff cloud accounts (e.g., Google Workspace or Microsoft 365).

- **Role-Based Access Control (RBAC):** Access to Management Information Systems (MIS) like SIMS is strictly restricted based on current job descriptions.
- **Vendor Risk Assessment:** Individual academies cannot procure new software or cloud learning platforms without a formal **Data Protection Impact Assessment (DPIA)** approved by the central DPO.
- **Device Security:** All Trust-owned laptops and devices are centrally managed.

7. Centralised Subject Access Requests (SARs)

While a Subject Access Request may be submitted directly to an individual academy, it is legally a request to the Trust.

- **Coordination:** The receiving academy must notify the central DPO within **24 hours** of receipt. This email should be sent to both dpo@alet.org.uk and dposervicesltd@outlook.com
- **Response Timeline:** The central DPO will coordinate the collection of data across all relevant platforms and issue the statutory response within **one calendar month**.
- **Scope:** The search will include local academy records, central Trust emails, and any third-party software platforms used by that student or staff member.

8. Personal Data Breaches

A personal data breach at any member academy must be managed systematically:

- **Local Escalation:** The individual who discovers the breach must notify their Headteacher and the central DPO immediately on dpo@alet.org.uk and dposervicesltd@outlook.com . Confidential data transmitted to this email should be fully encrypted and/or password protected.
- **Containment:** The local ICT lead or central IT team will take immediate steps to mitigate the leak (e.g., recalling an email, locking an account).
- **Assessment:** The central DPO evaluates the risk to individuals' rights and freedoms.
- **ICO Notification:** ICO notification is required when a breach is likely to result in a risk to individuals' rights and freedoms. These breaches must be reported to the ICO within 72 hours of the Trust becoming aware of the breach.

Direct notification to affected individuals is required when the breach is likely to result in a high risk to individuals' rights and freedoms.

9. Policy Review & Dissemination

This policy is reviewed **annually** by the Trust Board in consultation with the DPO. Any updates are automatically pushed down to all member academies, requiring immediate adoption.

ACTIVATE LEARNING EDUCATION TRUST

Central vs. Local Responsibilities

Area	Central Trust Responsibility	Local Academy Responsibility
Policies & Privacy	Drafts, updates, and approves the master policy and templates.	Displays localised privacy notices on the school website.
Software Procurement	Reviews and signs off on DPIAs for new tech platforms.	Submits proposed systems to the DPO before purchasing.
Data Breaches	Investigates, records, and reports breaches to the ICO.	Reports all incidents to the central DPO within 24 hours. Investigates as directed/agreed at a school level.
Staff Training	Provides mandatory annual GDPR e-learning modules.	Ensures 100% staff completion during inset days.