Planet Education Networks

Data Retention Schedule

Approval Control

Document Title:	Data Retention Schedule
Approving Body:	Senior Leadership Team ("SLT")
Policy Lead:	Data Protection Officer ("DPO")
Last Review:	January 2025
Effective From:	February 2025
Next Review:	January 2026

Planet Education Networks

Contents

1. Introduction and Purpose

Planet Education Networks ("PEN") is committed to ensuring that personal data is not kept for longer than is necessary for the purposes for which it was collected. This Data Retention Schedule provides the framework for the secure and timely disposal of personal data across the PEN group.

The purpose of this schedule is to:

- Ensure compliance with the UK GDPR and the Data Protection Act 2018.
- Minimise the risk of holding excessive, outdated, or irrelevant information.
- Improve data management efficiency and reduce storage costs.
- Enable the organisation to respond accurately and efficiently to information requests.

2. Scope

This schedule applies to all personal data processed by PEN in its role as a Data Controller for its corporate functions and as a Data Processor providing services to its sister institutions. All staff and affiliated entities within the PEN group are required to adhere to this schedule.

3. General Principles

- **Compliance:** Retention periods are determined by legal, statutory, and operational requirements.
- **Minimisation:** Data will be retained only for as long as necessary to fulfil the purpose for which it was collected.
- **Secure Destruction:** At the end of the retention period, data will be securely and irreversibly destroyed (e.g., shredding, secure electronic deletion).
- **Review:** This schedule will be reviewed annually to ensure it remains current with legal and operational changes.

4. Data Retention Periods

The following table outlines the standard retention period for key categorised data.

Data Category	Example Types of Data	Standard Retention Period	Legal and Operational Justification
Student & Academic Records			
Student Enrolment Records	Application forms, offer letters, student contracts	6 years after the end of the academic year of enrolment or last contact.	Contractual obligation, limitation periods for legal claims.
Student Academic Transcripts & Awards	Final transcripts, degree certificates, award details	Permanently.	To provide a lifelong record of academic achievement and verify awards.
Student Module & Assessment Records	Mark sheets, coursework, exam scripts	1 year after the publication of final award, to allow for appeals.	Operational requirement for the appeals process.
Student Disability & Support Records	Reasonable adjustment agreements, support plans	6 years after the end of study.	Equality Act 2010 obligations, potential for disability-related claims.
HR & Staff Records			
Employee Personnel Files	Contract, salary, role history, performance reviews	6 years after the end of employment.	Limitation Act 1980 (contractual claims), HMRC requirements.
Recruitment Records (Unsuccessful Candidates)	CVs, application forms, interview notes	1 year from the end of the recruitment process.	To defend against potential discrimination claims under the Equality Act 2010.
Payroll & Pension Records	Payslips, P60s, pension contributions	7 years from the end of the tax year.	HMRC legal requirement.
Accident Reports & RIDDOR Records	Reportable injury records	7 years from the date of the report.	Health and Safety at Work etc. Act 1974.
Financial & Operational Records			
Financial Accounts & Ledgers	Invoices, purchase orders, expense claims	7 years from the end of the financial year.	Companies Act 2006, HMRC requirements.

Contractual Agreements	Supplier contracts, partnership agreements	6 years after the contract expiry or termination.	Limitation Act 1980 (breach of contract claims).
IT System Logs & Backups	Access logs, system event logs, backup tapes	Backups: 3 months (regular cycle). Critical Security Logs: 2 years.	Operational recovery and investigation of security incidents.
Marketing & Communications			
Website Enquiry Data	Contact form submissions, prospect data	2 years from last meaningful contact, unless consent is withdrawn earlier.	Legitimate interests for relationship management.
CCTV Footage	Security camera recordings	30 days, unless required for an active investigation.	ICO guidance, legitimate interests for security.

5. Responsibilities

- **Heads of Department:** Are responsible for ensuring that staff within their area are aware of and comply with this schedule.
- **Data Protection Officer ("DPO"):** Is responsible for maintaining and reviewing this schedule, providing guidance, and overseeing its implementation.
- **All Staff:** Are responsible for managing the data they process in line with this schedule and for ensuring secure disposal at the end of the retention period.

6. Secure Disposal Methods

At the end of the retention period, data must be disposed of securely and irreversibly:

- Paper Records: Must be cross-shredded or placed in confidential waste bins for professional destruction.
- Electronic Data: Must be deleted such that it cannot be easily recovered. This includes using secure deletion software or services that overwrite the data. Simply moving a file to the computer's recycle bin is not sufficient.
- Hard Drives & Media: Must be physically destroyed or professionally wiped using methods that meet recognised standards (e.g., NCSC guidelines)

7. Review and Exceptions

This schedule will be reviewed annually by the DPO. Exceptions to these retention periods may be made in specific circumstances, such as:

- An ongoing legal or regulatory investigation.
- A subject access request or other legal hold.
- An active business need that requires the data to be retained for a defined, short-term period beyond the standard timeframe.

Any such exception must be documented and approved by the DPO.

Contact for Queries:

For any questions regarding this Data Retention Schedule, please contact the Data Protection Officer at ashlea.b@pengroup.com.