Planet Education Networks

Data Protection and Confidentiality Policy

Approval Control

Document Title:	Data Protection and Confidentiality Policy
Approving Body:	Senior Leadership Team (“SLT”)
Policy Lead:	Data Protection Officer (“DPO”)
Last Review:	September 2025
Effective From:	October 2025
Next Review:	September 2026

Planet Education Networks

Contents

1. Introduction

Planet Education Networks ("PEN") is committed to protecting the privacy and security of personal data. We are a data controller under the Data Protection Act 2018 ("DPA 2018") and the UK General Data Protection Regulation ("UK GDPR").

This Policy outlines how we comply with our legal obligations and ensures that all staff, students, and third parties understand their roles and responsibilities in protecting personal data.

2. Purpose and Scope

This Policy applies to all personal data processed by PEN, regardless of the format or medium. It applies to all staff members (including permanent, temporary, and contracted staff), governors, contractors, consultants and agents. Any breach of this policy may result in disciplinary action.

3. Roles and Responsibilities

- **SLT:** Ultimately accountable for ensuring PEN's compliance with data protection law.
- **Heads of Departments:** Are responsible for ensuring staff within their area comply with this policy, developing local procedures, and promoting a culture of data protection.
- **DPO:** Responsible for monitoring compliance, advising on data protection obligations, providing training, acting as the primary contact for the ICO and data subjects, and overseeing PEN's information governance framework, including record keeping and data protection impact assessments. The DPO can be contacted at ashlea.b@pengroup.com.
- **All Staff:** Are responsible for complying with this policy, handling personal data securely, and reporting data breaches immediately.

4. Data Protection Principles

PEN processes personal data in accordance with the seven data protection principles, requiring that data shall be:

a. Processed lawfully, fairly, and transparently.

b. Collected for specified, explicit, and legitimate purposes.

c. Adequate, relevant, and limited to what is necessary.

d. Accurate and, where necessary, kept up to date.

e. Kept in a form which permits identification of data subjects for no longer than is necessary.

f. Processed in a manner that ensures appropriate security.

g. PEN is responsible for, and must be able to demonstrate compliance with, these principles (Accountability).

Our Privacy Notice, available on our website, provides clear information on how we collect, use, and share personal data.

5. Data Subject Rights and How to Exercise Them

Under data protection law, data subjects have the following rights, which are not absolute and may be subject to specific conditions:

- The right to be informed
- The right of access

- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Making a Subject Access Request ("SAR"): To exercise your rights, particularly the right of access, please submit a request in writing to the Data Protection Officer at ashlea.b@pengroup.com. We will respond to your request within one month of receipt.

6. Responsibilities of all Data Users

Staff who process personal data must:

- Ensure they have a lawful basis for processing, as defined in the UK GDPR and Appendix B.
- Handle special category data with extreme care, ensuring both a lawful basis and an additional condition for processing under Article 9 (see Appendix C).
- Complete mandatory data protection training.
- Use only approved and compliant systems for processing personal data.
- Keep personal data secure and not disclose it to anyone without authorisation.
- Report any actual or suspected data breaches immediately using the process in Section 11.

7. Responsibilities of Employees

All employees are responsible for providing accurate and up-to-date personal information to PEN and informing the relevant department (e.g., Admissions, Registry, HR) promptly of any changes.

8. Data Sharing and Transfers

- **Data Sharing:** Personal data will only be shared with third parties where there is a lawful basis to do so. Data sharing agreements and Data Protection Impact Assessments (DPIAs) will be used where required. For detailed procedures, staff should consult the DPO.
- **International Transfers:** PEN transfers limited categories of personal data to its sister company in Bangladesh for operational purposes, specifically for the provision of HR, Admissions, and IT support services.
    - Bangladesh is not covered by a UK adequacy regulation. Therefore, we ensure the transfer is lawful by implementing the UK International Data Transfer Agreement (IDTA), which provides appropriate safeguards for the data.
    - Data subjects are informed of this transfer and the safeguards in place through our Privacy Notice.
    - No staff member may transfer personal data internationally without prior consultation with and authorisation from the DPO.

9. Recordkeeping and Confidentiality

PEN maintains records for administrative, academic, and welfare purposes. All personal information is treated with sensitivity and confidence. It will only be used for the purposes for which it was collected and will not be disclosed to third parties without the data subject's express written permission, except where:

- There is a legal obligation (e.g., a court order or statutory requirement).
- There is a credible and significant risk of serious harm to the data subject or another person, and disclosure is a necessary and proportionate response.
- The data has been anonymised for statistical reporting.

10. Disposing of Personal Data

Personal data will not be retained for longer than is necessary. It will be securely destroyed or erased in accordance with the PEN's Records Retention Schedule and other relevant retention policies. The DPO will advise on the secure disposal of data.

11. Data Breach Management

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff and students must report any actual or suspected data breach immediately upon discovery. The Data Incident Reporting Form (Appendix D) must be completed and sent to ashlea.b@pengroup.com. PEN has a duty to report certain breaches to the ICO within 72 hours. Failure to report a breach may result in disciplinary action.

12. Making a Complaint

Data subjects have the right to make a complaint about how their personal data is handled. Complaints should first be raised with the PEN's DPO at ashlea.b@pengroup.com. If unsatisfied with the response, a complaint can be lodged with the Information Commissioner's Office (ICO) at https://ico.org.uk/make-a-complaint/.

13. Equality Statement

This policy will be applied in a manner consistent with the Equality Act 2010, ensuring no less favourable treatment based on protected characteristics.

14. Related Regulations, Policies and Procedures

This policy should be read in conjunction with, but is not limited to, the following:

- External:
  - Data Protection Act 2018
  - UK General Data Protection Regulation (UK GDPR)
- Internal:
  - Privacy Notice
  - Student Records Retention Schedule
  - Information Security Policy

15. Review of the Policy

This Policy is owned by the DPO and will be reviewed annually by the SLT, or sooner in response to changes in legislation.

Appendix A

Definitions

This section provides definitions and explanations of important terms related to data protection.

Anonymisation and Pseudonymisation	Are methods used to protect personal data by either completely removing identifiers or separating them from the data.
Consent	Is the freely given, specific, informed, and unambiguous indication of a data subject's wishes for the processing of their personal data.
Data Controller	Is the individual or organisation responsible for ensuring compliance with data protection laws and determining the purpose and means of data processing.
Data Processors	Are individuals or organisations that process personal data on behalf of the data controller.
Data Protection Impact Assessment ("DPIA")	Is a tool used to identify and reduce risks in processing activities.
Data Protection Officer	Is appointed to advise on data protection obligations, monitor compliance, and act as a point of contact with regulatory authorities.
Data Subjects	Refers to an individual to whom personal data relates and who can be identified from that data.
EEA	Refers to the 28 countries in the European Union and Iceland, Lichtenstein, and Norway.
Personal Data	Refers to any information that can identify a natural person, and special category personal data includes sensitive information that requires extra protection.

Appendix B

The Lawful Bases for Processing Personal Data

This section explains the six lawful bases for processing personal data under the UK GDPR, including consent, contract, legal obligation, vital interests, public task, and legitimate interests. The six lawful bases for processing personal data under the UK GDPR are consent, contract, legal obligation, vital interests, public task, and legitimate interests.

Consent must be freely given, specific, informed, and unambiguous, and require a positive opt-in. Processing personal data is necessary for a contract or to take specific steps before entering into a contract. Processing personal data is necessary to comply with the law, protect someone's life, perform a task in the public interest, or for legitimate interests.

Appendix C

The Lawful Bases for Processing Special Categories of Personal Data

The lawful bases for processing special categories of data are outlined in Article 9 of the UK GDPR and supplemented by conditions in the Data Protection Act 2018. When processing special categories of data, at least one condition from Article 6 and one from Article 10 of the UK GDPR must be met. These conditions include explicit consent, protection of vital interests, legal claims, public interest, and healthcare purposes.

Appendix D

Incident Reporting Form

One must act promptly to report any data breaches (or potential data breaches/near miss). If a data breach or near-miss is discovered, the relevant head of division/department must be notified, and a completed form (below) returned to ashlea.b@pengroup.com.

Description of breach:	
Time data breach was identified and by whom:	
Time data breach occurred and by whom:	
Who is reporting the breach?	
Name/post/department:	
Email address:	
Classification of data breached (in accordance with the breach policy): Public data Internal data Restricted data Confidential data	
Volume of data involved (number of people affected):	
Is the breach contained or ongoing?	
What actions are being/have been taken to recover the data?	
Any other relevant information:	