

Information Security & Hosting Overview

SMID (by Prodeo Ltd)

Last updated: February 2026

1. Purpose of this document

This document provides an overview of the technical and organisational measures used by **Prodeo Ltd** to protect personal data processed within **SMID**, our assessment and tracking platform for UK schools.

It is intended to support:

- school Data Protection Impact Assessments (DPIAs)
- due diligence by Data Protection Officers (DPOs)
- IT and safeguarding reviews
- procurement and assurance processes

This document should be read alongside:

- the SMID Privacy Notice
 - the Data Processing Agreement
 - the List of Sub-processors
-

2. Roles and responsibilities

For the purposes of UK GDPR:

- **Schools** using SMID act as **Data Controllers**
- **Prodeo Ltd** acts as a **Data Processor**, providing the platform and related support services

Prodeo Ltd processes personal data only on the documented instructions of the school and in accordance with applicable data protection legislation.

3. Overview of the SMID platform

SMID is a secure, cloud-hosted web application designed to help schools:

- analyse and report on pupil progress

- monitor attainment and assessment data
- support educational planning and intervention

SMID is used exclusively within the UK education context and is provided only to schools.

4. Hosting and infrastructure

4.1 Core hosting providers

SMID is hosted using enterprise-grade cloud infrastructure provided by the following suppliers:

- **Amazon Web Services (AWS)**
Used for core infrastructure, data storage and managed services.
- **Heroku (a Salesforce company)**
Used for application hosting, deployment and operational management.
- **Snowflake**
Used for secure backend data storage and analytics.

These providers are widely used across the UK public sector and education technology sector and operate robust security, resilience and compliance programmes.

Further detail on the underlying security controls operated by key cloud and infrastructure providers is provided in **Appendix A**.

4.2 MIS data integrations (Wonde)

Where authorised by the school, SMID may receive data via Wonde, a specialist education data integration provider used by many UK schools.

Wonde acts on the school's instructions to securely extract data from the school's Management Information System (MIS) and transmit it to SMID.

Prodeo Ltd does not control the school's MIS or Wonde's platform and receives only the data that the school has authorised to be shared. Data transferred via Wonde is encrypted in transit and subject to contractual safeguards.

4.3 Hosting model

- SMID is deployed within logically isolated environments.

- Infrastructure is managed in accordance with a recognised **shared responsibility model**:
 - cloud providers secure the underlying infrastructure
 - Prodeo Ltd is responsible for application-level security, configuration and access controls

Hosting is **UK- and EU-targeted by default**.

5. Use of AI services (OpenAI)

5.1 Purpose and scope

SMID includes optional features that allow authorised users to submit text to an AI service to generate summaries.

Key characteristics:

- AI use is **user-initiated**
- Users decide when and how to use AI features
- AI is not required for core SMID functionality
- Schools and users retain control over the data they choose to submit

Prodeo Ltd does **not** require or encourage the use of pupil personal data within AI features and advises users to avoid entering such data.

5.2 OpenAI as a sub-processor

- SMID uses the **OpenAI API**, not consumer ChatGPT services.
- OpenAI acts as a **restricted sub-processor**.
- Data submitted via the API is used solely to generate the requested response.

Prodeo Ltd has configured the OpenAI service such that:

- data retention is disabled
- data is not used for model training
- processing is limited to the specific request made by the user

The output generated by the AI service is returned directly to the requesting user and is not shared with other users by default.

5.3 Data transfer considerations

Where AI features are used, data submitted may be processed outside the UK or EU. Such processing is:

- limited in scope
- initiated by the user
- subject to appropriate contractual safeguards in line with UK GDPR requirements

There are **no routine or automated transfers** of personal data outside the UK or EU as part of core SMID hosting.

6. Data categories and minimisation

SMID is designed to support data minimisation:

- only data required for assessment and reporting is processed
- schools control what data is uploaded
- special category data is not required for core functionality
- users are encouraged to avoid uploading unnecessary or sensitive information

Prodeo Ltd does not independently determine what pupil data is uploaded to SMID.

7. Technical security measures

Prodeo Ltd implements a range of technical controls to protect data processed within SMID, including:

7.1 Encryption

- encryption in transit using **TLS 1.2 or higher**
- encryption at rest using cloud provider-managed encryption mechanisms

7.2 Access controls

- role-based access control (RBAC)
- user access restricted to data relevant to their role
- separation of customer environments

7.3 Authentication

- secure password requirements
- protection against unauthorised access
- optional integration with single sign-on (SSO) where supported

7.4 Network security

- firewalls and network-level protections
 - restricted access to infrastructure components
 - monitoring of network activity
-

8. Organisational security measures

8.1 Staff access

- Prodeo Ltd staff access to live data is strictly limited
- access is granted only where necessary for support or maintenance
- access is logged and auditable

8.2 Training and awareness

- staff involved in service delivery are aware of data protection obligations
- access is reviewed regularly

8.3 Policies and procedures

- documented security and data protection practices
 - incident response procedures
 - regular review of controls
-

9. Monitoring, logging and audit

- system activity and access events are logged
 - logs support monitoring, troubleshooting and incident investigation
 - administrative actions are auditable
-

10. Backup, resilience and availability

- automated backups are performed
 - data is protected against accidental loss
 - infrastructure is designed for high availability
 - multi-zone resilience is provided by underlying cloud platforms
-

11. Incident management and breach response

Prodeo Ltd maintains procedures to identify, assess and respond to security incidents.

In the event of a personal data breach:

- the issue is investigated promptly
 - affected schools are notified without undue delay
 - relevant information is provided to support the school's own regulatory obligations
-

12. Data retention and deletion

- data is retained for the duration of the school's contract
- on termination, data can be exported by the school
- data is securely deleted from live systems and backups within agreed timeframes (typically within three months)

Further detail is available in the Data Retention & Deletion Policy.

13. Sub-processors

Prodeo Ltd uses a limited number of sub-processors to deliver SMID, including:

- Amazon Web Services (AWS) – cloud infrastructure and hosting
- Heroku (Salesforce) – application hosting and operational management
- Snowflake – secure data warehousing and analytics
- Wonde – MIS data integration (where authorised by the school)
- OpenAI – optional, user-initiated AI text summarisation features

Each sub-processor is subject to contractual obligations consistent with UK GDPR requirements, including appropriate technical and organisational measures.

A current list of sub-processors, including purposes and safeguards, is published as part of Prodeo Ltd's Trust & GDPR documentation and is available on request.

14. Review and assurance

This document is reviewed periodically and updated to reflect changes in the service, suppliers, or regulatory guidance.

Schools may use this document as supporting evidence within their DPIA and ongoing assurance processes.

Appendix A

Cloud & Infrastructure Security Controls (Summary)

This appendix provides additional information on the security controls operated by key third-party infrastructure and integration providers used in the delivery of SMID. It is intended to support DPIAs and technical assurance reviews.

A.1 Amazon Web Services (AWS)

Amazon Web Services (AWS) provides the core cloud infrastructure used to host SMID.

Key security characteristics include:

- AWS operates data centres with **multi-layered physical security**, including controlled access, monitoring, and environmental protections.
- AWS maintains internationally recognised security certifications, including:
 - ISO/IEC 27001 (information security management)
 - ISO/IEC 27017 (cloud security)
 - ISO/IEC 27018 (protection of personal data in the cloud)
- AWS provides independent assurance through **SOC 1, SOC 2 and SOC 3** reports.
- Data stored within AWS-managed services is **encrypted at rest by default**, with encryption keys managed by AWS.
- Data transmitted between services and user devices is protected using **TLS encryption**.

- AWS operates under a **shared responsibility model**, under which AWS secures the underlying infrastructure while Prodeo Ltd is responsible for application-level security and access controls.
-

A.2 Heroku (Salesforce)

Heroku is used for application hosting and operational management and is a platform operated by **Salesforce**.

Key security characteristics include:

- Heroku inherits security controls from Salesforce's enterprise security framework.
 - Salesforce maintains recognised certifications and assurance reports, including ISO 27001 and SOC reports.
 - Heroku provides:
 - managed patching and platform updates
 - logical isolation between applications
 - controlled administrative access
 - Security monitoring and vulnerability management are handled at the platform level, with application-level security managed by Prodeo Ltd.
-

A.3 Wonde (MIS data integration)

Where authorised by a school, SMID may receive data via **Wonde**, a specialist education data integration provider.

Key security characteristics include:

- Wonde acts only on the **explicit authorisation of the school**.
 - Data is transferred securely from the school's MIS using **encrypted connections**.
 - Only the data fields authorised by the school are shared.
 - Prodeo Ltd does not have direct access to the school's MIS and receives data only via the approved integration.
-

A.4 Snowflake (Data warehousing and analytics)

SMID uses Snowflake, an enterprise-grade cloud data platform, to support secure data warehousing and analytics as part of the SMID service.

Key security characteristics include:

- Snowflake operates under contractual data protection terms and acts only on the instructions of Prodeo Ltd.
 - Data stored within Snowflake is protected using encryption in transit and at rest.
 - Access to Snowflake environments is restricted and controlled by Prodeo Ltd through role-based access controls.
 - Snowflake provides platform-level security controls appropriate for regulated sectors, with infrastructure security managed by the provider and application-level controls managed by Prodeo Ltd.
 - Snowflake does not use customer data for training purposes; data retention and deletion are controlled by Prodeo Ltd in line with contractual and policy requirements.
-

A.5 Shared responsibility model

SMID is delivered using a shared responsibility model:

- **Infrastructure providers** (such as AWS, Salesforce/Heroku Wonde, and Snowflake) are responsible for the security of the underlying platforms and services they operate.
- **Prodeo Ltd** is responsible for:
 - application security
 - configuration and access controls
 - user management
 - data handling within SMID
- **Schools** remain responsible for:
 - deciding what data is uploaded
 - managing user access
 - meeting their obligations as Data Controllers

This model reflects standard practice for cloud-hosted services used within the UK education sector.