Education Technology Consultancy

Data Governance, Privacy and Security Overview

Consultant: Simon Dass
Role: Education Systems & Learning Technology Consultant
Location: Melbourne, Australia

1. Purpose of This Document

This document outlines the data governance, privacy and security principles used when designing or implementing education technology systems for schools and educational organisations.

The purpose is to provide transparency regarding:

- how student information may be handled
- where data is stored
- who owns and controls that data
- how systems are designed to protect privacy

The consultancy approach prioritises **privacy-by-design**, **data minimisation**, and **school ownership of information**.

This document may be provided to school leadership teams, IT departments, or governance bodies when evaluating new digital systems.

2. Consultancy Scope

The consultancy provides services including:

- learning data system design
- intervention and adjustment tracking systems
- workflow tools for teachers
- analytics dashboards for school leadership
- AI-assisted documentation tools
- professional learning and staff training

Where software tools are implemented, the focus is on **supporting school workflows**, not extracting or centralising student data.

3. Core Data Governance Principles

The consultancy operates under the following principles:

1. School Ownership of Data
Schools retain full ownership and control of their student information.

2. Data Minimisation
Systems are designed to collect only the information required for educational workflows.

3. Privacy by Design
Privacy considerations are embedded into the architecture of systems from the beginning.

4. Transparent Architecture
System structure, hosting and data flows are clearly documented for schools.

4. Data Ownership Model

A core principle of the consultancy is that:

Schools retain full ownership and control of their data.
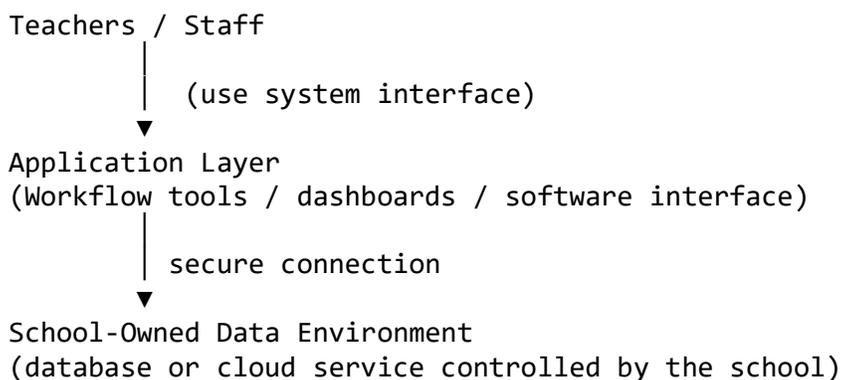
Where possible:

- databases are hosted within the school's own environment
- student data is not centrally stored by the consultant
- the consultant does not retain copies of school data

This approach ensures that schools maintain authority over:

- student information
- access permissions
- data retention policies
- compliance with institutional privacy frameworks

5. Typical System Architecture

Most systems implemented through this consultancy follow a structure similar to the diagram below.

```
Teachers / Staff
        |
        |   (use system interface)
        ▼
Application Layer
(Workflow tools / dashboards / software interface)
        |
        |   secure connection
        ▼
School-Owned Data Environment
(database or cloud service controlled by the school)
```
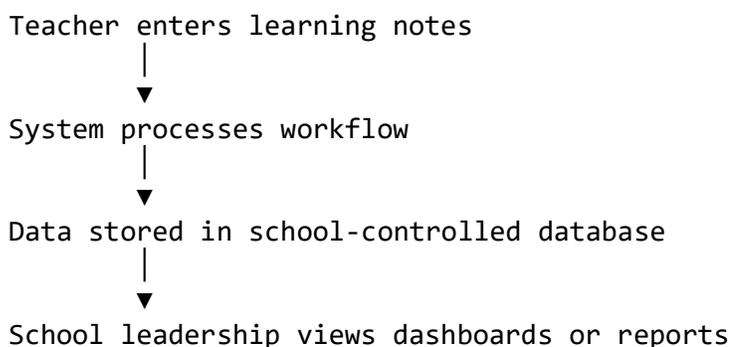
In this structure:

- the **school hosts the database**
- the **software provides the interface**
- the **consultant does not store student data externally**

This architecture significantly reduces privacy risks associated with third-party software vendors.

6. Data Flow Model

A simplified data flow is illustrated below.

```
Teacher enters learning notes
        |
        ▼
System processes workflow
        |
        ▼
Data stored in school-controlled database
        |
        ▼
School leadership views dashboards or reports
```

Key characteristics of this model:

- student information remains inside school infrastructure
- systems act as workflow tools rather than data warehouses
- schools retain full control over access and retention

7. Data Minimisation

Systems designed through this consultancy follow a **minimal data model**.

Only the information necessary to support educational workflows is collected.

Examples of information that may be used include:

- student first name or identifier
- learning adjustment records
- intervention tracking
- curriculum or learning notes
- teacher observations

Sensitive information such as full student records, addresses, or personal identifiers should remain within existing school management systems.

8. Hosting Environments

Systems may be implemented within a variety of school-controlled environments, including:

- Microsoft 365 / SharePoint
- school-managed cloud environments (Azure, Google Cloud, etc.)
- school-hosted databases
- locally hosted servers

The goal is to ensure that **schools maintain technical and legal control over their data infrastructure**.

9. Privacy-by-Design Approach

Systems implemented through this consultancy are designed around privacy-first architecture.

Key practices include:

- minimal collection of personal information
- role-based access control
- separation between application layers and data layers
- transparent system architecture

Where AI or automation tools are used, care is taken to ensure that:

- sensitive student information is not unnecessarily transmitted to external services
- data is anonymised or minimised where appropriate

10. Alignment with Australian Privacy Frameworks

System design is informed by recognised privacy frameworks used across Australian education environments.

These include:

- Australian Privacy Principles (APPs)
- state education department privacy requirements
- institutional school privacy policies

Design decisions typically support principles such as:

- collecting only necessary information
- protecting personal information through secure system design
- enabling schools to maintain control of their data

11. Information Security Practices

Security practices used when designing systems include:

- secure authentication methods
- role-based access control
- encrypted connections (HTTPS)
- restricted database permissions
- separation between application and data layers

Security practices are informed by widely recognised standards such as **ISO 27001 information security principles**.

12. Roles and Responsibilities

Consultant Responsibilities

The consultant is responsible for:

- system architecture design
- configuration of software tools
- technical documentation
- training and professional learning
- supporting schools during implementation

School Responsibilities

Schools remain responsible for:

- hosting environments
- management of student data
- access permissions
- compliance with organisational privacy policies

13. Professional Practice

The consultancy operates with the goal of supporting schools to implement technology in a way that:

- reduces teacher workload
- improves visibility of learning support
- protects student privacy
- aligns with existing school policies

Technology should support education, not complicate it.

14. Contact

Simon Dass
Education Systems & Learning Technology Consultant

Melbourne, Victoria, Australia

For enquiries regarding consultancy services or system design approaches, please contact directly.