exposé
A Synechron Company

Exposé Case Study

*Solution providing a trusted view of technology usage and cyber risk across schools, improving governance and cybersecurity compliance.*

# Education – Information Stewardship Reporting

# Education: Information Stewardship Reporting

CASE STUDY

**Automated Information Stewardship reporting solution providing a single, trusted view of technology usage and cyber risk across schools, improving governance, reducing manual reporting effort, and strengthening cybersecurity compliance at scale.**

## PROBLEM

A leading education provider supporting schools across the state required a reliable and consistent way to understand, manage, and assess the technologies in use across individual sites. This capability was critical to meeting the objectives of a state-level Cyber Security Framework, particularly in identifying cyber risk, assessing technology suitability, and ensuring compliance with ICT standards.

Prior to this initiative, technology assessments and insights were maintained in manually curated Excel spreadsheets. This approach was time-consuming, difficult to maintain, and prone to user error, with limited scalability. It also reduced visibility, consistency, and confidence in reporting, making it challenging for schools and central education offices to gain a clear, trusted view of their technology landscape and associated cyber risks.

## SOLUTION

To address this challenge, an automated Information Stewardship Report was developed using the Enterprise Data Warehouse (EDW) to replace manual, spreadsheet-based processes. Data is extracted via APIs from JAMF (Apple applications) and Microsoft Defender (cloud and Windows applications) using Azure Data Factory (ADF) pipelines driven by control tables and platform identification. This provides a consistent, repeatable, and scalable method for identifying active technologies across schools.

The solution progressed from a proof of concept into a production reporting capability that delivers secure, role-based views. Schools can see only their own technology snapshot, while ICT and education offices access an aggregated view of assessed technologies, including risk classifications, usage restrictions, and required controls. Ongoing mass refreshes and progressive updates ensure the report remains current and aligned with cybersecurity governance processes.

The report provides clear visibility of approved, restricted, and unsupported technologies, enabling informed decision-making by schools. Linking technologies to risk classifications and required controls improves compliance and governance alignment.

## BUSINESS BENEFITS

- Reduced manual effort and reliance on spreadsheets, eliminating error-prone processes and improving data accuracy across all schools.
- Enabled ICT teams to save significant time previously spent collating and validating technology information, allowing resources to be redirected to higher-value cybersecurity and operational initiatives.
- Improved visibility of technology usage across schools, enabling faster identification of high-risk, undesirable, or prohibited technologies.
- Strengthened cybersecurity governance by providing a single, trusted source of truth aligned to the state-level Cyber Security Framework.
- Accelerated technology assessment and decision-making for schools by clearly identifying supported, restricted, and unsupported technologies.
- Enhanced executive and stakeholder confidence through accurate, repeatable, and auditable reporting on technology risk and compliance.