EDTECH ESSENTIAL DUE DILIGENCE CHECKLIST

Don't buy an edtech product without asking these critical questions of your vendor:

SECURITY MEASURES

- Where is the data hosted and by whom?
- Does the company certify your data remains in Australia?
- Is all data encrypted in transit?
- Is all data encrypted at rest?
- Are user profiles encrypted in transit?
- Are user profiles encrypted at rest?
- How often does the company conduct penetration testing? To what standard? (e.g. Open Web Application Security Project, OWASP)

DATA ACCESS

- Does the solution include access controls to ensure only authorised staff have access to your data?
- Does the company conduct security training for staff to prevent inadvertent disclosures?
- Do all staff in the company with access to your data hold current relevant child protection checks?
- Has the company provided details of all third parties providing services and/or support for the product or otherwise have access to your data?
- What physical access controls are in place at the locations from which data may be stored or accessed?
- Does the company have an internal data management and handling policy?
- Does the company have a published Notifiable Data Breach Plan?
- Has the company ever had a data breach? How long ago?

COMPLIANCE

- Have you audited the product's functional processes and procedures to ensure compliance with your legal obligations?
- Does the company have procedures to destroy or retrieve personal information, in compliance with the Information Privacy Act 2000 with Privacy Act 1988 (Cth).
- Does the company regularly review audit logs?
- Does the company regularly conduct reviews of user access levels?

QUALITY CONTROL

- Has the company implemented change control processes to minimise disruption during business hours?
- Does the company have a Business Continuity Plan in the event of a natural disaster?
- Does the solution use data loss prevention technologies?
- What is the Recovery Time Objective?
- What is the Recovery Point Objective?
- Does the company make the data available to the customer in an agreed format upon request?
- How long does the company retain data for?
- Does the company securely delete the data upon the customer's request and certify that deletion?

edsmart.com