Privacy Breach Notification Process

School Administration Services Limited trading as EasyBus

Version: 1.0
Date: April 2026
Owner: Greig Neilson, Network Manager
Next review: April 2027

1. Purpose

This document sets out the steps EasyBus takes when a privacy breach occurs or is suspected. It is designed to ensure EasyBus meets its obligations under the Privacy Act 2020, including the requirement to notify the Privacy Commissioner of notifiable privacy breaches within 72 hours.

2. What is a privacy breach

A privacy breach is any unauthorised or accidental access to, disclosure, alteration, loss, or destruction of personal information held by EasyBus. Examples include:

- a student record being sent to the wrong parent
- unauthorised access to the EasyBus platform database
- a laptop or device containing student data being lost or stolen
- a third party gaining access to EasyBus systems without authorisation
- accidental deletion of personal information

3. What makes a breach notifiable

Not all breaches require notification to the Privacy Commissioner. A breach is notifiable if it is likely to cause serious harm to the affected individuals. Factors that indicate serious harm include:

- the information relates to a child or young person
- the information includes home addresses, health information, or behavioural records
- the breach involved deliberate or malicious access
- a large number of individuals are affected
- the information could be used to locate, identify, or harm an individual

Given that EasyBus holds home addresses, school attendance records, and health information for children, most significant breaches will be notifiable. When in doubt, treat the breach as notifiable.

4. Response steps

The following steps apply immediately upon discovering or suspecting a privacy breach.

STEP 1 · Immediately

Contain the breach

– Stop any ongoing unauthorised access — disable compromised accounts, revoke API keys, or take affected systems offline if necessary.
– Preserve evidence — do not delete logs, emails, or records related to the breach.
– Identify what information was involved and how many individuals are affected. The platform audit log (activity_log) and Supabase Auth / Postgres logs are the primary tools for this.

STEP 2 · Within 4 hours

Assess the breach

– Determine whether the breach is likely to cause serious harm (see Section 3).
– Identify the cause — human error, system failure, or malicious act.
– Document findings: what happened, when, what data was involved, and who is affected.

STEP 3 · Within 24 hours

Notify affected individuals

– Contact affected parents or guardians directly by email or phone.
– Explain what information was involved, what happened, and what steps EasyBus is taking.
– Advise them of what they can do to protect themselves.
– Do not delay individual notification pending the Privacy Commissioner notification.

STEP 4 · Within 72 hours

Notify the Privacy Commissioner

– File a notification at www.privacy.org.nz using the online breach notification tool.
– Include: the nature of the breach, the types of information involved, the number of individuals affected, and the steps taken to contain and remediate.
– If 72 hours is not enough time to gather full details, file an initial notification and supplement it as further information becomes available.

STEP 5 · Within 7 days

Remediate and review

– Address the root cause of the breach.
– Update system access controls, policies, or procedures as needed.

– Document the full incident record including timeline, notifications sent, and remediation steps.
– Review whether changes to the EasyBus platform or internal processes are required to prevent recurrence.

5. Key contacts

Contact	Role	Contact details
Greig Neilson	Network Manager, EasyBus	privacy@easybus.nz
Privacy Commissioner	Office of the Privacy Commissioner	privacy.org.nz · 0800 803 909
Supabase	Database and auth provider	supabase.com/support

6. Record keeping

Every breach, whether notifiable or not, must be documented. The incident record must include: the date and time the breach was discovered, a description of what occurred, the types of information involved, the number of individuals affected, the steps taken to contain the breach, whether notification was made to the Privacy Commissioner and when, and any remediation actions taken.

Incident records are retained for seven years in accordance with the EasyBus Data Retention Policy.

7. Policy review

This process is reviewed annually or following any breach event. Next review due April 2027.