



INCIDENT RESPONSE PLAN

Word Labs Education

Version 1.0 · March 2026

Owner	Nicholas Deeney, Word Labs Education
Contact	nick@wordlabs.app
Website	wordlabs.app

1. PURPOSE

This plan defines how Word Labs Education will detect, respond to, and recover from security incidents, particularly those involving personal information. It ensures compliance with the **Notifiable Data Breaches (NDB) scheme** under the Australian Privacy Act 1988.

2. SCOPE

This plan covers:

- Unauthorised access to student or teacher data
- Data breaches (accidental or malicious disclosure of personal information)
- System compromise (application, database, or infrastructure)
- Denial of service or extended outage affecting data availability
- Loss or corruption of data

3. INCIDENT SEVERITY LEVELS

Critical — Immediate response (within 1 hour)

Confirmed breach of personal information; data exfiltrated or publicly exposed.

Examples: database dump leaked, auth bypass exploited, student data exposed.

High — Response within 4 hours

Likely breach or active attack in progress; personal data at risk.

Examples: suspicious database queries, unauthorised admin access detected.

Medium — Response within 24 hours

Potential vulnerability discovered; no confirmed data exposure.

Examples: XSS vulnerability reported, RLS misconfiguration found.

Low — Response within 72 hours

Minor issue with no data exposure risk.

Examples: cosmetic bug, non-sensitive logging issue.

4. INCIDENT RESPONSE TEAM

Given Word Labs is a sole-trader operation, the response team is:

Role	Person	Contact
Incident Lead	Nicholas Deeney	nick@wordlabs.app
Technical Support	Supabase Support	support@supabase.io
Payment Security	Stripe Support	stripe.com/support

For incidents requiring specialist expertise, an external security consultant will be engaged as needed.

5. DETECTION

Automated monitoring

- **Supabase Dashboard:** Database query logs, auth logs, API request logs
- **Vercel Analytics:** Traffic anomalies, error rate spikes

- **Stripe Dashboard:** Payment anomalies, disputed transactions
- **Browser errors:** Client-side error reporting via console logs (manual review)

Manual monitoring

- Regular review of Supabase auth logs for failed login attempts
- Review of database RLS policy effectiveness
- Teacher-reported issues via feedback form or email

Indicators of compromise

- Unusual number of failed teacher login attempts
- Database queries accessing data outside normal patterns
- Unexpected changes to RLS policies or database schema
- Reports from teachers of data they shouldn't be able to see
- Spike in Edge Function invocations (potential API abuse)

6. RESPONSE PROCEDURES

Step 1: Contain (Immediate)

Goal: Stop the breach from worsening.

Action	How
Disable compromised teacher accounts	Supabase Auth — disable user
Revoke Supabase anon key (if RLS bypassed)	Supabase Dashboard — Settings — API — Rotate anon key
Take application offline (if critical)	Vercel Dashboard — pause deployment
Rotate Edge Function secrets	Supabase Dashboard — Edge Functions — Secrets
Block suspicious IPs	Vercel Firewall / Supabase network settings

Step 2: Assess (Within 4 hours)

Goal: Determine what happened and what data was affected.

1. Review Supabase database logs for the incident timeframe
2. Review Supabase Auth logs for unauthorised access
3. Identify which tables/rows were accessed or modified

4. Determine if personal information was accessed (student names, teacher emails)
5. Determine the root cause (vulnerability, misconfiguration, credential compromise)
6. Document findings in an incident log

Step 3: Notify (Within 30 days — NDB scheme)

Under the Notifiable Data Breaches scheme, if the incident involves an **eligible data breach** (unauthorised access to personal information likely to result in serious harm), Word Labs must notify:

3a. Notify the OAIC

- **Who:** Office of the Australian Information Commissioner
- **When:** As soon as practicable, within 30 days of becoming aware of the breach
- **How:** Submit via the OAIC Notifiable Data Breach form ([oaic.gov.au](https://www.oaic.gov.au/ndb))
- **Include:** Description of the breach, types of information involved, number of individuals affected, steps taken to contain, recommended steps for affected individuals

3b. Notify affected individuals

- **Who:** All teachers whose data was affected; schools (as data controllers) for student data
- **When:** At the same time as the OAIC notification, or as soon as practicable
- **How:** Email to affected teacher accounts; letter/email to school principals for student data
- **Include:** What happened, what data was involved, what we're doing about it, what they should do (e.g., change passwords), contact details for questions

3c. Notify schools (for student data)

- Schools are the data controllers for student information
- Contact the school principal and IT coordinator directly
- Provide the school with information needed for their own incident response and parent communication

Step 4: Remediate

1. Fix the root cause vulnerability
2. Deploy the fix to production
3. Verify the fix resolves the vulnerability (test with the same attack vector)
4. Review related code/configuration for similar vulnerabilities
5. Update security architecture document if the architecture changed

6. Update RLS policies if authorisation was the issue

Step 5: Review (Within 2 weeks)

1. Conduct a post-incident review
2. Document lessons learned
3. Update this incident response plan if needed
4. Implement additional monitoring to detect similar incidents
5. Consider whether external penetration testing is warranted

7. DATA BREACH ASSESSMENT CRITERIA

Under the NDB scheme, a breach is notifiable if:

1. There is **unauthorised access to, or disclosure of, personal information** held by Word Labs, AND
2. A **reasonable person would conclude** that the access/disclosure would be **likely to result in serious harm** to any of the affected individuals

Serious harm factors

- The type of personal information involved (names, emails, passwords)
- The sensitivity of the information (children's data is treated as more sensitive)
- Whether the information is protected by security measures (encryption, access controls)
- The nature of the harm that could result (identity theft, discrimination, psychological)
- The individuals affected (children require higher protection)

Word Labs data risk assessment

Data type	Risk level	Notes
Student data (first names)	Low re-identification risk	Treated as sensitive due to age (9–12); first names only, no surnames or other PII
Teacher data (email addresses)	Moderate risk	Potential phishing or spam
Game progress (scores)	Non-sensitive	Accuracy percentages and play time

Data type	Risk level	Notes
Payment data	Not applicable	Not held by Word Labs — processed by Stripe

8. COMMUNICATION TEMPLATES

Template: Teacher notification email

Subject: Security Notice — Word Labs

Dear [Teacher Name],

We are writing to inform you of a security incident affecting your Word Labs account.

What happened: [Brief description]

When: [Date/time of incident]

What data was involved: [Specific data types]

What we have done: [Steps taken to contain and fix]

What you should do:

- Change your Word Labs password immediately
- [Any other recommended actions]

We have reported this incident to the Office of the Australian Information Commissioner as required under the Notifiable Data Breaches scheme.

If you have questions, please contact nick@wordlabs.app.

Sincerely,
Nicholas Deeney
Word Labs Education

Template: School principal notification

Subject: Data Incident Notification — Word Labs

Dear [Principal Name],

We are writing to notify you of a security incident that may affect student data associated with your school's Word Labs account.

What happened: [Brief description]

What student data was involved: [First names, game progress — specify exactly]

What we have done: [Steps taken]

As the data controller for your students' information, you may wish to:

- Inform affected parents/guardians
- Review your school's own incident response procedures

Please note that Word Labs only stores student first names and game progress data.

No surnames, emails, dates of birth, or other personally identifiable information is stored.

We have reported this to the OAIC. A copy of our report is available on request.

Contact: nick@wordlabs.app

Sincerely,

Nicholas Deeney

Word Labs Education

9. RECORD KEEPING

All incidents (regardless of severity) will be recorded with:

- Date and time of detection
- Description of the incident
- Severity level
- Data affected (if any)
- Actions taken
- Root cause (once identified)
- Resolution date
- Whether OAIC notification was required and made

Records will be retained for a minimum of **5 years** as per Australian Privacy Principles.

10. PLAN REVIEW

This plan will be reviewed:

- Annually (at minimum)
- After any security incident
- When the application architecture changes significantly
- When privacy legislation changes

11. CONTACT

Incident Lead	Nicholas Deeney
Email	nick@wordlabs.app
Security architecture	wordlabs.app/security-architecture
Privacy policy	wordlabs.app/privacy
External regulator (OAIC)	oaic.gov.au · 1300 363 992
NSW IPC	ipc.nsw.gov.au · 1800 472 679

Last reviewed: March 2026. This plan will be reviewed annually or after any security incident.