



**Te Tāhuhu o
te Mātauranga**
Ministry of Education

Phillip Fry

fyi-request-33483-51af222a@requests.fyi.org.nz

26/03/2026

Tēnā koe Phillip

OIA: GEMS-46484 – SMART data governance

Thank you for your email of 10 January 2026 to the Ministry of Education (the Ministry), subsequently clarified on 28 January 2026, requesting the following information:

I request the following information relating to governance and oversight of access to student data within the Student Monitoring, Assessment and Reporting Tool (SMART):

1. *Copies of any formal access control documentation relied upon by the Ministry for SMART, including:*
 - *role-based access control (RBAC) specifications or access matrices; and*
 - *documentation describing differences in data access between user roles (e.g. teachers, principals, Ministry staff, Janison staff, and subcontractors).*
2. *Documentation describing whether SMART data access for each role is:*
 - *identifiable at the individual student level, or*
 - *restricted to aggregated or de-identified views.*
3. *Copies of any formal policies or assurance documents describing audit logging and monitoring of access to SMART data, including:*
 - *who can view audit logs; and*
 - *how inappropriate access or misuse is detected and managed.*

This request is limited to formal, authoritative documents and does not seek informal correspondence or draft material.

Your request has been considered under the Official Information Act 1982 (the Act).

In response to **parts one** and **two** of your request, and as provided for under section 16(1)(e) of the Act, please find attached, as **Appendix A**, a summary of the Role-based

Wellington – National Office, PO Box 1666, Wellington 6140
Phone: +64 4 463 8000

[education.govt.nz](https://www.education.govt.nz)

access control (RBAC) specifications relied on by the Ministry for SMART. As you will see, this includes a table classifying each role by whether it is intended to access identifiable student-level information, only aggregated/de-identified views, or (for students) their own records for participation.

With regard to **part three** of your request, I am withholding the Ministry's *formal policies or assurance documents describing audit logging and monitoring of access to SMART data, including how inappropriate access or misuse is detected and managed*, under section 6(c) of the Act, as releasing this information would be likely to prejudice the maintenance of the law, including the prevention, investigation and detection of offences. Releasing these documents could enable malicious actors to evade detection, exploit system behaviours, and/or compromise security safeguards.

However, with regard to your particular points of interest, we can advise as follows:

- *who can view audit logs*

Access is controlled via authorised administrators, namely Janison Cyber Security and Data Protection Team and the Ministry's Cyber Security Operations Team.

- *how inappropriate access or misuse is detected and managed.*

Inappropriate access or misuse is detected and managed through a monitoring process that includes the following steps:

1. Detect
2. Triage
3. Investigate
4. Respond
5. Review

Please note, we may publish this response on our website after five working days. Your name and contact details will be removed.

Thank you again for your email. You have the right to ask an Ombudsman to review my decision on your request, in accordance with section 28 of the Act. You can do this by writing to info@ombudsman.parliament.nz or to Office of the Ombudsman, PO Box 10152, Wellington 6143.

Release

Nāku noa, nā

Pauline Cleaver

Hautū | Deputy Secretary

Te Poutāhū - Curriculum Centre