# PRIVACY IMPACT ASSESSMENT

Updated, March 2023

This Privacy Impact Assessment relates to the My School Election web-based application for the use of Returning Officers managing online school board elections in New Zealand.

My School Election is owned by  EducationPlus Auckland Ltd., responsible for the preparation and publication of this report.

This report assesses the My School Election web-based application against the 13 Information Privacy Principles (IPP) included in the Privacy Act 2020.

# Privacy Principle 1: PURPOSE OF COLLECTING PERSONAL INFORMATION

This principle provides that personal information should only be collected if it is for a lawful purpose, and is necessary for that purpose.

Our response:

- The information required for the preparation of the Electoral Roll is

| ***PURPOSE OF THE INFORMATION*** | **WHAT PERSONAL INFORMATION?** |
|---|---|
| *For purchase of the licence to use* | Returning Officers: required information<br>Name<br>School<br>Mobile phone number |
| *For preparation of the electoral roll (Parent representative election)* | Parents and caregivers:<br>Name,<br>Postal address<br>Email address<br>Mobile phone number |
| *For preparation of the electoral roll (Staff representative election)* | Staff:<br>School email address, OR working email address |
| *For preparation of the electoral roll (Student representative election)* | Students:<br>School email address |
| *For candidate management and to meet the data requirements of the Ministry of Education* | Candidates: required information<br><br>Name<br>Postal address<br>Email address<br>Mobile phone number<br>Name of nominator<br>Email contact of nominator<br>Phone contact of nominator |
| | Candidates: optional information<br><br>Gender<br>Ethnicity<br>Previous governance history<br><br>Profile picture<br>Candidate statement |
| *For electronic voting purposes and authentication* | Unique identifier (User Code)<br>Mobile phone number<br>Password |

## Privacy Principle 2: SOURCE OF PERSONAL INFORMATION

This principle provides that personal information should only be collected directly from the person concerned (unless there are specific exceptions).

### Our response:

- Voter personal information for the electoral roll is provided by the school or returning officer client in .csv or Excel form and sourced from a school's Student Management System (SMS). There is no interoperability with school systems.

- Schools construct the information required from enrolment information. This information may change over time. A school's enrolment process will normally include permissions for the use of the information for school-related activities. A school board election may be a specified activity. Information for the purposes of board elections is an activity permitted under the regulations and the legislation, and is a school-related activity.

- Contributing primary schools to an Intermediate are required to release information about parents and caregivers of Year 6 students for the purpose of establishing an Electoral Roll for their (in-zone) intermediate school. (Education and Training Act 2020 Schedule 22 (1) (1) ).

- The Returning Officer dashboard does not link to any school database, and the information supplied for the electoral roll is not linked to any other information.

- Candidate personal information is provided by candidates through the nomination process. Candidates must approve the use of the information they supply for election purposes.

- Returning officer information and/or user contact details are provided by the client school.

## Privacy Principle 3: DISCLOSURE OF PERSONAL INFORMATION

This principle provides that people whose personal information is being used should be aware that the information is being collected about them, why it is being collected and who will be using it.

People should be able to contact the agent collecting the information about them, be able to find out where and how their information is being stored, know the law under which the information is being collected and used, whether the information is mandatory or voluntary, know the consequences for not allowing the Returning Officer to use the information, and their rights to access and correction.

### Our response:

- The My School Election Privacy Policy is publicly available on our website and provided to school clients and Returning Officers to share with their community. The Privacy Policy specifies what information is being collected and why.

- The electoral roll contains only the information required for the conduct of a postal or electronic election according to school election regulations.

- *Access to the full electoral roll* is limited to the Returning Officer and administrative personnel.

- *The public version of the electoral roll* is limited to the names of those eligible to vote as required by the election regulations.

- The disclosures required by IPP3 are included in communications sent from the application by the Returning Officer. The electronic email Call for Nominations -
    - Names the Returning Officer / Āpiha Whakahoki for the election.
    - Specifies the reason why a parent of a student at a contributing school is on the roll.
    - Checks with the recipient whether the data provided is correct.
    - Provides an opt-out channel.
    - Describes how to access the Electoral Roll through a "more details" link.

## Privacy Principle 4: MANNER OF COLLECTION OF PERSONAL INFORMATION

This principle provides that people whose personal information is being collected should not be unduly coerced into providing it.

### Our response:

- Under the terms of our software licence, Returning Officers are required to follow the Privacy Policy of their schools and the My School Election Privacy Policy, and to follow Standard Operating Procedures as outlined in the User Guide.

- Only the information as outlined in IPP1 of this report is required to conduct an election.

- The candidate nomination form clearly identifies which statistical information for the Ministry of Education is optional and which is required for the purpose of the election. Candidates authorise the use of the information for election purposes.

- Use of the election management application prohibits the use of the application for unlawful purposes.

## Privacy Principle 5: STORAGE AND SECURITY OF PERSONAL INFORMATION

This principle requires that every precaution is taken to ensure that personal information is protected against loss, misuse or disclosure, including when it is in transit and when it is being stored.

### Our response:

| Data state | Response |
|---|---|
| **Data in transit** | We invite school clients to use DropBox, OneDrive, or other proprietory equivalents to securely transfer information via .csv or excel file. |
| | (In the case of postal voting method) transmissions are via secure direct upload to the mailing house. |
| **Data in use** | Access to the My School Election application / dashboard requires valid Multi Factor Authentication (MFA).<br>Voter data held on our servers is encrypted.<br>User and Administrator activity is logged.<br>Data access events to the management dashboard and the voting platform are logged. |

| | |
|---|---|
| | Working files are held in password-protected folders on our OneDrive computer system. |
| | We use password-protected and MFA access to our OneDrive system to prepare electoral roll data for upload to the MySchoolElection dashboard (Full Service clients).<br><br>Returning Officers sourced by schools prepare electoral roll data for upload to the MySchoolElection dashboard on internal school systems or by separate arrangement. |
| | Standard Operating Procedures apply to data in use (available in the My School Election User Guide) |
| **Data in storage** | Voter passwords are stored as secure, brute force resistant hash values.<br>Voter Unique Identifiers (see IPP 13) are stored as secure, brute force resistant hash values.<br>We do not hold personal information in storage (see IPP 9). |
| | We have an Incident Response policy which ensures that client schools are immediately informed of data breaches. |

## Privacy Principals 6 and 7: ACCESS TO and CORRECTION OF PERSONAL INFORMATION

These principles require that personal information, once disclosed, can also be readily retrieved, can be confirmed, ensure that the person can have access to it and request correction of it.

### Our response:

- The personal information we hold (see IPP1) is shared with each voter through the Call for Nominations (see IPP3). A voter can request corrections or removal through an immediate response button (Also IPP3).
- Information amended on our system may also be amended by the Returning Officer on the school database.
- Where a Returning Officer does not have access to the school database, the person requesting correction will be referred back to the school as the source of the incorrect data.

## Privacy Principle 8: CHECKING PERSONAL INFORMATION BEFORE USE

This principle requires us to take reasonable steps to ensure that the information Returning Officers use is accurate, up to date, complete, relevant and not misleading.

### Our response:

- Returning Officers rely on school data quality management systems for accuracy and relevance.
- As a Returning Officer, we apply sense checks to the data provided, and refer any obvious issues – such as missing postcodes or obvious gaps - back to client schools.

## Privacy Principle 9: NOT KEEPING PERSONAL INFORMATION LONGER THAN NECESSARY

This principle states that personal information can only be kept for the purpose it was required, and not longer.

### Our response:

- The regulations require us to maintain access to records for up to 60 days before transferring required documents to the District Court.
- Returning Officers have a licence to use the software for a specified period, after which any data remaining on the My School Election application will be electronically destroyed by our administrator.
- As a Returning Officer, we provide written confirmation to schools that their information has been removed from the application and from our computer systems.

## Privacy Principle 10: LIMITS ON THE USE OF PERSONAL INFORMATION

This principle states that we can only use personal information for the purpose it was collected, and not otherwise.

### Our response:

- We only use information for election purposes. We do not provide information to third parties.
- Returning Officers only have access to the information for the schools for which they hold a licence. They may only use the information for election purposes.

## Privacy Principle 11: LIMITS ON DISCLOSURE OF PERSONAL INFORMATION

This principle states that we must not disclose personal information unless we have reasonable grounds to believe it falls within specified exemptions.

### Our response:

- We do not provide information to third parties.
- Returning Officers are required to follow school privacy policy and the My School Election Privacy Policy.

## Privacy Principle 12: OVERSEAS DISCLOSURE OF PERSONAL INFORMATION

This principle states that we may only disclose personal information overseas if the recipient of this information has privacy obligations similar to New Zealand.

### Our response:

- We do not provide information to third parties, including to any overseas parties; except for our mailing house (postal voting purposes only)

- Returning Officers are required to follow both school privacy policy and the My School Election Privacy Policy.

## Privacy Principle 13: UNIQUE IDENTIFIERS

This principle requires that unique identifiers cannot be used unless required to carry out our functions efficiently.

### Our response:

- The requirements of a ballot are that it be secret, valid, and secure. A User Code is assigned to voters when the Electoral Roll is imported to the Returning Officer dashboard. The User Code can only be used once to complete the ballot.

- Once a ballot is completed, a receipt is issued. The receipt number is used for auditing purposes, and does not identify the voter.