NSW Electoral Commission

LG.220A

# Candidate request for list of electors for Non-Client Councils

*Clause 284A, Local Government (General) Regulation 2021*

## Candidate details

SURNAME

GIVEN NAME(S)

ENROLLED ADDRESS

SUBURB/TOWN

STATE/TERRITORY

POSTCODE

PERSONAL EMAIL ADDRESS (REQUIRED TO RECEIVE ENROLMENT INFORMATION ELECTRONICALLY)

MOBILE NUMBER

**Contest:** (please tick one)

☐ MAYOR ☐ COUNCILLOR

**Certified photo ID attached:**

☐ Yes

A certified copy of a photo ID (e.g., drivers licence or passport) must be attached to this form. If we cannot verify who you are, access will be refused.

COUNCIL AREA/WARD (IF APPLICABLE)

DD / MM / YYYY

ELECTION DATE

## Candidate declaration

I, the above named candidate, have read the attached information sheet titled *Important information for the safeguard of enrolment information*. I understand my obligations as detailed in the information sheet, which include the following:

- I am only permitted to use the enrolment information I wish to receive solely for a purpose in connection with the election for the local government area, in which I am a candidate.
- I must **not** disclose enrolment information in any form to any other person or entity, unless the disclosure would be a use of the information that is permitted under the *Local Government (General) Regulation 2021* ("LG Regulation").
- I must **not** use enrolment information for a commercial purpose.
- I must maintain systems and procedures that are adequate to preserve the security of enrolment information.
- I will notify the NSW Electoral Commission if I become aware of, or if I suspect that there has been, any data breach concerning enrolment information.
- I must destroy the encrypted data file containing the enrolment information and erase/destroy all data copied from it immediately following the declaration of the election.

In signing this declaration, I am requesting that enrolment information be provided to me by the Electoral Commissioner in accordance with clause 284A of the LG Regulation. I understand that the list of electors contains enrolment information which is protected information and is subject to sections 51 and 52 of the *Electoral Act 2017* (as applied and modified by clauses 284B and 284C of the LG Regulation, respectively). These legislative provisions prescribe strict limitations and restrictions on the use and disclosure of enrolment information. I also understand that my failure to comply with a protected information provision is an offence under the Act and may result in significant monetary penalties (maximum of 1000 penalty units/$110,000).

I have also read and understood the *Information collection notice* on this form located on page 2 of this form.

SIGNATURE OF CANDIDATE

DD / MM / YYYY

DATE

This form must be signed and returned by email (see Submitting the completed form and certified copy of photo ID on page 5.

## Information collection notice

The personal information on this form is collected and used by the Electoral Commission to undertake its statutory and administrative functions relating to elections. We may also use the contact details on this form to send you information or reminders or to provide feedback about interactions with us. We may at our sole discretion make public statements that you are a recipient of a list of electors, including in media statements and in response to concerns or questions raised by relevant stakeholders, such as electors who may make complaints to us about your use of enrolment information. This form is held by the Electoral Commission and accessible by relevant staff and its contractors. The information on this form may also be disclosed to other government agencies and as otherwise authorised or required by law. Your failure to complete this form may result in your request being delayed or refused. You can find additional information concerning access to your personal information in our Privacy Management Plan published on our website.

OFFICE USE ONLY

| | |
|---|---|
| RECEIVED BY | DD / MM / YYYY<br>DATE RECEIVED BY ENROLMENT SUPPORT |
| PROVIDED BY | DD / MM / YYYY<br>DATE PROVIDED TO CANDIDATE OR REPRESENTATIVE |

# Important information for the safeguard of enrolment information – local government candidates

*Clause 284A Local Government (General) Regulation 2021*

## Purpose

This information sheet provides guidance to candidates in general terms about the security and safeguard of enrolment information.

## Outline of candidates' responsibilities for safeguarding enrolment information

This information sheet outlines the main responsibilities of candidates with respect to the safeguarding of enrolment information.

The NSWEC does not and cannot give legal advice to candidates about their specific circumstances. It is the responsibility of candidates to ensure that their use and disclosure of enrolment information is permitted under law.

In summary, candidates' obligations around safeguarding enrolment information include, but are not limited to, the following:

- they are only permitted to use the enrolment information provided solely for a purpose in connection with the election for the local government area, in which they are a candidate.
- they must **not** disclose enrolment information in any form to any other person or entity, unless the disclosure would be a use of the information that is permitted under the *Local Government (General) Regulation 2021* ("LG Regulation").
- they must not use enrolment information for a commercial purpose.
- they must **not** use enrolment information provided to another person or entity.
- they must maintain systems and procedures that are adequate to preserve the security of enrolment information.
- they must destroy the encrypted data file containing the enrolment information and erase/destroy all data copied from it immediately following the declaration of the election in which they are a candidate (this applies whether or not their nomination as a candidate is successful).

## What is enrolment information?

Enrolment information is also called protected information. It is the enrolment information provided by the Electoral Commissioner to candidates pursuant to clause 284A of the LG Regulation.

The Electoral Commissioner will provide candidates with a list of electors only for the ward or, if the area is not divided into wards or the candidate is a mayoral candidate for the area, a list of electors for the area in which the candidate is running for election.

## How can candidates use enrolment information?

A candidate may only use the enrolment information provided for a purpose in connection with the election for the local government area, in which they are a candidate ("permitted use").

## What uses of enrolment information are prohibited?

The use of enrolment information that is not solely for a purpose in connection with an election in which a person is a candidate is prohibited.

Candidates must also cease using enrolment information as soon as the election is declared (whether or not their nomination as a candidate is successful).

If candidates unlawfully use enrolment information they may be subject to significant monetary penalties. Section 51 of the *Electoral Act 2017* (NSW) ("Electoral Act") (as applied and modified by clause 284B of the LG Regulation) prescribes a maximum penalty of 1000 penalty units/$110,000.

For example using enrolment information for the following purposes are strictly prohibited (below is not an exhaustive list):

- ascertaining the personal details of individuals who make public statements in support of or in opposition to particular candidates or political parties on social media;
- any purpose after the declaration of the election;
- undertaking functions pertaining to a council;
- undertaking functions pertaining to a councillor or mayor;
- contacting family, friends and/or lost acquaintances;
- curiosity;
- sharing information with other persons or entities including other candidates and/or party members;
- financial gain;
- employment purposes;
- commercial purposes;
- to sell or offer to sell enrolment information;
- augmenting mailing lists;
- sending birthday cards and other messages not relevant to the election in which they are a candidate.

## Can candidates disclose enrolment information to other persons or entities?

Candidates must not disclose enrolment information to any other person or entity, unless the disclosure would be a use of the information for a permitted use under the LG Regulation.

If candidates unlawfully disclose enrolment information they may be subject to significant monetary penalties.

Section 52 of the Electoral Act (as applied and modified by clause 284C of the LG Regulation) prescribes a maximum penalty of 1000 penalty units/$110,000.

If candidates intend to engage a service provider to assist in the carrying out of a permitted use e.g. a mailing house, they should ensure that any arrangement entered into with that service provider for a permitted use will, as a minimum:

- require the service provider to have and maintain adequate systems and procedures with respect to the security of enrolment information;
- require the service provider to keep enrolment information private and confidential at all times;
- prohibit the service provider from copying enrolment information for the provider's own purposes;
- require the service provider to use enrolment information only for a permitted use;
- require any subcontractors of the service provider to agree to the same obligations as the service provider;
- enable the candidate to control how the enrolment information is handled by the service provider;
- require the service provider to return enrolment information to the candidate for destruction at the completion of the contracted service.

## Are there minimum IT system requirements that candidates should take to protect enrolment information?

Candidates must take all necessary precautions to prevent loss, unauthorised access to, unauthorised copying, misuse, modification or disclosure of enrolment information. The following list is intended as a guide only and is not exhaustive. Candidates are personally responsible for ensuring IT systems are adequate at all times.

- Candidates should only download or access the enrolment information using an electronic device belonging to them – access to or downloading of enrolment information from a public computer (such as a computer belonging to an internet café) is not secure.
- Ideally, an electronic device should only be used for a permitted use. If this is not possible, candidates should remain vigilant in relation to cyber security for the device and take appropriate security measures to protect enrolment information. These measures include ensuring applications and web browsers on the device are configured for maximum security, so as to prevent access to malicious websites that may download malware designed to steal data stored on their electronic devices.
- Candidates' electronic devices used to access or download the enrolment information should not be connected to an insecure or publicly available internet connection. Public WiFi services sometimes offered for free in shops or hotels, is not considered a secure internet connection. Personal wireless connection used by candidates must be set up with strong passwords.
- Candidates' devices should have an appropriate log-in setup/configuration to prevent unauthorised access to the device.
- Candidates' devices should only be used by the candidate and must not be shared with any other persons unless it is a device that authenticates individual users and the other users cannot access the enrolment information provided to the candidate.
- Candidates' devices should authorise automatic security updates and candidates should regularly check that such updates have successfully installed onto the device.
- Candidates' devices should have a reputable antivirus and malware protection solution with latest definitions installed.
- Candidates should adopt commonly accepted cyber security measures such as locking electronic devices when not in use and strong passwords for log-ins (including multi-factor authentication).
- Screen sharing – Ensure you are not sharing your screen while accessing the enrolment information
- Candidates should ensure that all other devices that may be connected to their shared network are secure by following common security measures.
- Candidates should regularly monitor the operation and effectiveness of their security measures to ensure that they remain responsive to changing threats and vulnerabilities and other issues that may impact the security of enrolment information.
- Candidates should ensure the security codes required to access or download the enrolment information are secure and not shared.
- Candidates should keep enrolment information encrypted and password protected at all times.
- After the election is declared, candidates must destroy the encrypted data file and erase/destroy all data copied from it. Candidates should, amongst other things consider all possible devices that have been used to access enrolment information and all possible ways in which enrolment information may have been saved and/or transmitted (for example software applications, databases, emails, local/cloud archives and backups) to ensure all enrolment information is appropriately deleted in such a manner as to prevent its retrieval.

## What should a candidate do if there is a data breach?

Candidates must **immediately** notify the NSW Electoral Commission by email (ncc.rolls@elections.nsw.gov.au) if they become aware of, or if they suspect that there has been, any data breach concerning enrolment information and take all reasonable steps to stop that breach and/or further breaches. In addition, a candidate should report the breach to NSW Police if the cause of the data breach is the result of cybercrime, fraud, theft or other illegal activity.

A candidate may wish to obtain their own legal advice in the event of a data breach that involves enrolment information, including as to any possible obligations under the Mandatory Notification of Data Breaches Scheme. See What happens if there are specific questions about a candidate's circumstances? of this information sheet.

## Will the NSW Electoral Commission investigate a data breach?

The NSW Electoral Commission is empowered to institute proceedings for offences under the LG Act in connection with the conduct of local government elections. A data breach will be assessed for possible review and investigation. If the data breach concerns an offence that involves the conduct of another regulatory agency, the NSW Electoral Commission will consult with that agency (see the NSW Electoral Commission's *Compliance and Enforcement Policy* published on its website).

## Will the NSW Electoral Commission notify the public of a data breach?

The NSW Electoral Commission may notify the Privacy Commissioner and/or impacted electors and make public statements or notifications about a data breach involving enrolment information held by a candidate. The NSW Electoral Commission may **identify a candidate as the recipient of the enrolment information** that was lost, unlawfully disclosed, unlawfully used or unlawfully accessed (whether the cause of the breach was the result of an act or omission of the candidate, third party or otherwise) in its communications to the Privacy Commissioner, affected/concerned individuals, the media and in public notifications or statements.

## Are there prohibitions or criminal offences about enrolment information that are found outside electoral laws?

All enrolment information is protected information and is subject to sections 51 and 52 of the Electoral Act (as applied and modified by clauses 284B and 284C of the LG Regulation, respectively) which prescribe limitations and restrictions on the use and disclosure of enrolment information. Failure to comply with these provisions may result in a maximum penalty of 1000 penalty units/$110,000.

There are also rules outside electoral legislation, however, concerning the collection, use, disclosure and security of personal information that may apply to candidates. These can be found in (but are not limited to) the *Privacy and Personal Information Protection Act 1998* (NSW), the *Crimes Act 1900* (NSW) and the *Independent Commission Against Corruption Act 1988* (NSW).

Failure to comply with relevant legislative provisions under these other Acts may also result in significant monetary penalties and/or terms of imprisonment for candidates.

## What do candidates need to do to obtain access to a list of electors?

To obtain access, a person must be nominated as a candidate for the election and only after the returning officer has nominated candidates under clause 295 of the LG Regulation and the election is to be a contested election – being registered as a candidate for campaign finance purposes under the *Electoral Funding Act 2018* is not sufficient to meet eligibility requirements.

- Candidates are required to complete the form **LG.220A Candidate request for list of electors for Non-Client Council**.
- Candidates are required to read the form and this information sheet.
- Candidates must attach a certified copy of their photo ID to the form.
- The completed form is to be signed and returned by email (see Submitting the completed form and certified copy of photo ID).
- Candidates must meet the full cost of any computer systems and/or programming required in the storage and/or use of enrolment information.

## Who can certify a candidate's photo ID

Persons with the following qualifications or occupations are eligible to certify the documents:

- Justice of the peace.
- Registered lawyer.
- Police officer.
- Postal manager.
- Registered or licensed medical practitioner, dentist, pharmacist or nurse.
- Veterinary surgeon.
- Certified practising accountant.

The certified copy must include the statement or words to the effect "I certify that this is a true copy of the original document as sighted by me". The certifier must also include their signature, full name, registration number (if any), qualification/ occupation and date on each of the certified documents.

## Submitting the completed form and certified copy of photo ID

Candidates must submit the completed form and certified copy of photo ID to the NSW Electoral Commission by email.

**By email:** Important note: Prior to submitting via email you must receive a Mimecast access key (password) from the NSW Electoral Commission. Mimecast is a secure way to send and receive emails. You can request an access key by emailing ncc.rolls@elections.nsw.gov.au or phoning 1300 135 736.

## In what manner and form will candidates be provided a list of electors?

- The Electoral Commissioner may provide the enrolment information in any particular manner or form.
- The enrolment information will be provided electronically.
- The provision of enrolment information is not ongoing.
- The Electoral Commission will not provide any technical/ IT support or data manipulation assistance.
- The Electoral Commissioner provides the enrolment information on an "as is" basis without warranty or acceptance of liability of any kind, including in respect of its quality, operability, accuracy or completeness.
- While the Electoral Commission takes all reasonable steps and safeguards concerning the security of its websites and systems, it accepts no liability or responsibility for any interference with or damage to candidates' computers, software or data occurring as a result of accessing the enrolment information.

## What happens if there are specific questions about a candidate's circumstances?

Independent legal advice should be sought if further information or advice is required in relation to the specific circumstances of a candidate who is seeking access to, or using or disclosing enrolment information.

Although the NSWEC cannot discuss matters subject to an investigation or provide legal advice it may be able to provide further information in general terms about the issues discussed in this information sheet.

Candidates may contact the Customer Service Team by phone 1300 135 736 or by email ncc.rolls@elections.nsw.gov.au.

This information sheet is provided for general guidance only, however, and does not limit the rights and remedies available to the Electoral Commissioner and other persons under relevant legislation in response to any actions or omissions by a candidate with respect to a candidate's use and/or disclosure of enrolment information.

## Accessing further information

If you are deaf, or have a hearing impairment or speech impairment, contact us through the National Relay Service. TTY users – phone 133 677 then ask for 1300 135 736. Speak and Listen users – phone 1300 555 727 then ask for 1300 135 736. Internet relay users – connect to the National Relay Service then ask for 1300 135 736.

If you need an interpreter, call TIS National on 131 450 and ask them to call the Electoral Commission on 1300 135 736. Business hours are 9am to 5pm, Monday to Friday.



LG.220A_EL_3787_JUN24_V8