

Guidance.



Standing as an election candidate.

If you are standing for election, you will use personal information about the people living in your constituency. This happens when you canvass, when you write to residents, and when you keep a record of who you have spoken to and what they said. Data protection law applies whenever you do this.

This guidance explains, in plain terms, what you need to do to use that information lawfully. More detailed guidance on every aspect of data protection is on our website at www.inforights.im.

In data protection law you are called the “**controller**”. That means you are responsible for the personal data you use for your campaign, and you must be able to show that you are using it properly.

The data protection principles

You must handle personal data in line with the principles set out in Article 5 of the Applied GDPR. In short, personal data must be:

1. used lawfully, fairly and in a way people would expect (lawfulness, fairness and transparency);
2. collected only for your stated purpose and not used for anything else (purpose limitation);
3. limited to what you actually need (data minimisation);
4. accurate and kept up to date (accuracy);
5. kept no longer than you need it (storage limitation); and
6. kept secure (integrity and confidentiality).

Underpinning all of these is accountability. You must be able to demonstrate how you meet them.

Take extra care with political opinions

Information about a person's political opinions is **special category data**, along with information about their health, sexual orientation, and racial or ethnic origin. It needs a higher level of protection. When you record how a resident intends to vote, or their views

on an issue, you are handling special category data, so keep it secure and use it only for your campaign.

People's rights

Residents have rights over their personal data, set out in Articles 13 to 22 of the Applied GDPR. These include the right to:

- know who you are and why you are using their personal data;
- ask you for a copy of the personal data you hold about them;
- object to you using it, including for canvassing;
- ask you to stop using it; and
- ask you to correct or delete it.

You must be ready to respond to these requests.

Keeping personal data secure

You must put appropriate measures in place to keep personal data safe. That means controlling who can see it, storing it securely, and not sharing it more widely than necessary. Take particular care with special category data, and with the electoral register.

Using AI tools and online services

Free and low-cost artificial intelligence (AI) tools, such as chatbots and writing assistants, are now widely available. It can be tempting to use them for campaign tasks, for example to draft letters, summarise responses, or sort through your canvassing records.

You must not put the electoral register, or any personal data about residents, into these tools.

When you type or upload information into a public AI tool, you generally lose control of it. The provider may store it, use it to train its systems, or process it on servers outside the Island. This means:

- You would be disclosing residents' personal data to a third party you do not control, for a purpose that has nothing to do with the election. That is very likely to break the law, including the rules on how the electoral register may be used.
- Information about how residents intend to vote, or their political views, is special category data. Putting this into an AI tool is a serious breach.
- You cannot guarantee the security of the data, and you usually cannot delete it once it has been entered, so you cannot meet your obligations as a controller.

You can still use AI tools for general tasks that do not involve anyone's personal data, for example drafting a standard leaflet, or checking the spelling and grammar of text that names no one. If you are in any doubt, do not enter the information.

Canvassing: letters, emails, calls and messages

UK case law has established that political canvassing is a form of **direct marketing**. This gives residents certain rights.

Addressed letters

Residents have the right to object to receiving letters addressed to them personally. If someone objects, whether verbally or in writing, you must not send them any further campaign material. Letters addressed simply to "The Owner/Occupier", and leaflet drops, are not personal data, so this right does not apply to them.

Emails and text messages

Under the **Unsolicited Communications Regulations 2005**, you must not send campaign emails or text messages to a resident unless they have already agreed to receive them.

Telephone calls

You must not telephone a resident to canvass support if their number is registered with the Telephone Preference Service, unless they have already agreed that you may call.

Using the electoral register

As a candidate, you are entitled to a copy of the full register of electors for the area in which you are standing, in paper or electronic form, to help you canvass. The supply and use of the register is governed by the **Registration of Electors Act 2020** and the **Registration of Electors Regulations 2021**. The full register contains the personal data of everyone registered to vote in that area, including their name and address.

Use the register only for the election

You may only use the register for purposes connected with the election. Using it for any other purpose, or passing it to anyone else for another purpose, is a criminal offence. Keep it separate from your other records, and do not merge it into general contact lists, mailing tools or marketing systems.

Sharing the register with others

You may give a copy of the full register to your appointed polling agents, counting agents and election agents, or to a supplier processing the information for your campaign, for example a company printing a personalised mailing. They must not use it for any other purpose, and you must make sure every copy is returned to you or securely destroyed when it is no longer needed.

Registering with the Commissioner

You must have a registration entry in your own name if you, or anyone acting on your behalf, use electronic equipment to process personal data for your campaign. This includes using any computer or device to canvass residents and record their views, or to generate personalised letters, emails or text messages, whether these are sent by you or on your behalf.

To receive the electoral roll you must also be registered with the Commissioner.

There is no fee to register. Your details will appear on the public register kept by the Commissioner. Failing to register when you are required to is an offence. You can register through our website at www.inforights.im.

After the election

If you are elected

You may keep your copy of the full register and the personal data relating to your campaign, such as names, addresses, contact details and recorded views. Your registration entry continues while you hold office and must be renewed (at no cost) each year.

If you are not elected

You no longer have a lawful reason to keep any personal data from the campaign, including your copy of the full register. You must securely delete all of it, and cancel your registration entry, once the result is known.

If someone complains

Residents can complain to the Commissioner about how you have handled their personal data. If they do, you are required to cooperate with any investigation.

The Commissioner's powers

The Commissioner monitors and enforces compliance with data protection law. This includes powers to take corrective and enforcement action, up to and including imposing a financial penalty.

Getting help

If you are unsure about anything in this guidance, contact us before you act.

Isle of Man Information Commissioner
PO Box 69, Douglas, Isle of Man, IM99 1EQ
Telephone: +44 1624 693260
Website: inforights.im
Email: ask@inforights.im