

The requirements of the Data Protection Act

The Data Protection Act (“DPA”) seeks to balance the legitimate need to process personal data with a person’s right to privacy and imposes certain obligations on data controllers such as the requirement to notify and to comply with the eight data protection principles when processing personal data.

Notification and the register entry

A candidate is required to notify the Information Commissioner (“Commissioner”) if they, or a third party acting on their behalf, process personal data for the purpose of the election using electronic equipment, such as a computer, or email, fax, sms messaging etc. Failure to notify is an offence.

A candidate can only claim an exemption from the requirement to notify if the candidate, or any third party acting on their behalf, does not use a computer, of any description, or any other form of electronic equipment to process personal data for the purposes of the election.

If you are required to notify you should contact the Commissioner’s office for the relevant documentation. No fee is payable for notification by a candidate.

Candidate’s details will then be included in a register entry which forms the publically available register maintained by the Commissioner. Successful candidates’ register entries will continue in force and must be renewed annually whilst they hold office. Unsuccessful candidates should cancel their register entry.

The Data Protection Principles

The DPA sets out rules to ensure that personal data is processed with due regard to the privacy and rights of individuals. These rules are the Eight Data Protection Principles. Candidates must comply with all the data protection principles irrespective of whether they are, or are not, required to notify.

The data protection principles apply to the processing by a candidate of all personal data, such as name, address etc. If a candidate records details of a constituent’s political views, opinions, or any indication of their voting intentions, this information is not only personal data, but is sensitive personal data. Additional safeguards must be in place to protect this information and it is important that sensitive personal data is destroyed securely at the end of the campaign.

Methods of canvassing

UK case law has established that political canvassing is a form of direct marketing. The DPA provides individuals with the right to object to such marketing.

If a candidate sends letters addressed to named constituents, those constituents have the right to ask the candidate to stop sending them direct marketing. If an individual has written to a candidate objecting to direct marketing then the candidate must not send any further material to that person.

Letters addressed to “The Owner/Occupier”, or leaflet drops, are not personal data and the above right does not apply.

Under the Unsolicited Communications Regulations 2005, candidates may not send emails or sms messages to a constituent to canvass support unless that constituent has previously agreed to

receive such messages. Similarly, candidates may not telephone a constituent to canvass support if that constituent's telephone number is registered with the Telephone Preference Service, unless that constituent has previously agreed to the candidate doing so.

Use of the Full Electoral Register

For the purposes of the election, a candidate is entitled to obtain a copy of the full register for the electoral area in which they are standing, either in hard copy, or in electronic format.

The supply and use of the full register is regulated by the Registration of Electors Act 2006 and associated Regulations. The full register contains the personal data, including name, address and, in certain cases, date of birth, of all constituents who have registered as being entitled to vote in a particular electoral area.

However, when registering to vote many constituents request that their details are not to be included on the edited register; i.e. they do not consent to the use of their personal details for any other purpose(s).

The full register therefore contains personal data that many constituents expect to remain confidential. It is the candidate's responsibility to ensure that these personal data are not used for any other purpose and failure to do so could result in the candidate being fined.

At the end of the election campaign, successful candidates may retain their copy of the full register; however, unsuccessful candidates no longer have a purpose for retaining the full register and should ensure that their copy is securely destroyed.

Provision of the full register to Third Parties

A candidate may provide a copy of the full register to

- appointed polling agents and counting agents;
- a processor for the purposes of processing the information for the election campaign e.g. to a company printing a personalised mail drop.

A third party may not use the copy of the full register for any other purpose and candidates must ensure that any copies they supply are returned to them and/or securely destroyed.