| Electoral Commission Search In this section Public notification of cyber-attack on Electoral Commission systems When you contact us When we contact you The electoral registers Electoral observers scheme Regulated entities Enforcement Applying for a job Cookies Election information and polling station finder Electoral Commission API Overview . In carrying out this work we collect and process personal information. This means we are a Data Controller under the regulations and we accept responsibility for ensuring we comply with all applicable requirements. We can be contacted at: The Electoral Commission 3 Bunhill Row London EC1Y 8YZ Our Data Protection Officer has appropriate knowledge and expertise to ensure compliance across all existing activities and to assess any new activities in this regard. For any queries about how we process personal data you can contact the Data Protection Officer: Andrew Simpson Data Protection Officer The Electoral Commission dataprotection@electoralcommission.org.uk Legal basis for processing personal data We process personal data to support the delivery of our statutory functions as set out in the Political Parties, Elections and Referendums Act 2000 and in support of the requirements of the Representation of the Peoples Act 1983 and subsequent regulations. These activities require us to process personal data that is necessary to perform a task in the public interest and in the exercise of official authority vested in the Electoral Commission as the Data Controller. There are some circumstances where we will ask for information that is not specifically referred to in legislation. These activities support our work and are therefore part of the delivery of our public task. These activities include, but are not limited to: contact made through our public information, election or regulatory telephone helplines information about your use of our website information provided by suppliers of good and services We will carry out further data processing to support corporate activities that do not have a basis in UK law, and these will be done under the legal basis that it is necessary for our legitimate interest. We have a legitimate interest in ensuring our organisation runs efficiently and this has wider societal benefits by ensuring we can carry out our public task. We undertake all processing under this basis proportionately and in a way that data subjects would expect. For example this will include procurement processes and publishing salary arrangements for senior staff in line with the UK Government’s transparency agenda. We do not make decisions by automated means using personal data or use the personal data you provide to us for any profiling purposes. Data Processors To support the delivery of key functions Data Processors process personal data on our behalf. These relationships are covered by contracts that ensure compliance with GDPR and UK data protection legislation. Examples of Data Processors include, but are not limited to: support providers to corporate systems call centre providers research partners payroll and pension providers Sharing personal data We may share personal data with other organisations for the delivery of a contract or in the delivery of our public task. The categories of recipients may include but are not limited to: police and prosecutory bodies Electoral Registration Officers Returning Officers other regulators (for example the Information Commissioner’s Office) Where we need to share information we will tell you who we need to share it with at the point of collection. When this is not possible we will take reasonable steps to contact you to advise you that we need to transfer data before that transfer. Retention of personal information Personal data will be kept only for so long as is necessary to fulfil the original purpose under which it was collected. At the point at which the data is no longer required it will be securely and safely disposed of. The criteria that we use to determine the period of retention takes into consideration various aspects including any legal requirement

to retain the information or any request from you, as the data subject, for erasure of the data. As a public body we are covered by the Freedom of Information Act 2000 (FOI). This means that we must respond to any requests for information within 20 working days unless exceptions apply. If a request under FOI includes personal data relating to you, we will anonymise this information to ensure that you cannot be identified by the information to be released. This means redacting information including your name, any descriptions or the identifiable information. If we consider that the release of personal data is necessary and appropriate when responding to the request then we will contact you before responding. We will ask for you to make representations regarding any reasons why you would not wish us to publish the information. We will endeavour to respect any such representation whilst meeting our obligations under the FOI Act. Your rights Your right to complain If you are at any point concerned or unhappy with the way in which we are processing your personal data, you may complain to the Information Commissioner's Office, via their online webform or telephone 0303 123 1113. Access to your information You have the right to request access to the information that we hold on you. This type of request is referred to as a subject access request. You can only request information about yourself and not that of others. To ensure that information is only released to the individual in question, we may ask you to confirm your identity when processing a request. This is likely to be in the form of a copy of photo ID (passport or driving license) and proof of address (utility bill). We will respond to a request of this type within one month of receiving the request. If we are unable to meet this timeframe, we will inform you of the delay within the month and the reasons for it. The maximum extension to the period for responding will be two months, bringing the total timeframe to three months. We will provide the information electronically wherever possible. There will be some circumstances where fully responding to your request may not be possible: If we hold a large volume of information relevant to your request, to the degree that it would hinder the fulfilment of the request within the statutory timeframe, we may ask you to define the nature for the information you want access to. This may, for example, be by refining subject matter or setting a timeframe for the information. If we hold the information for the purpose of the prevention, investigation, detection or prosecution of criminal offences we may not be able to provide you with access to your information. This may, for example, be relevant when we are holding information in relation to our enforcement case work or when information is shared with us by other law enforcement bodies. Restriction and rectification You have the right to request that we update or change any information that we hold that you deem is inaccurate, incomplete or no longer necessary, this is known as rectification. Restriction may be applied to processing whilst the accuracy or completeness of the information is being checked or if the purpose for which it is processed is being established. When making such a request you must set out the grounds or reasons relating to your particular circumstances that underlie your request. We will respond to requests unless there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or the establishment, exercise or defence of legal claims. If your personal data has been shared with any third parties, we will notify those third parties of your request for restriction or rectification and their responsibility to action your request. Objection and erasure You may object to the processing of your personal data. The right to object to processing means that you can request that we cease all processing of your data. This right cannot be applied to any information that is processed for the purposes of a legal obligation or the prevention, investigation,

detection or prosecution of criminal offences. You also have the right to request that we delete any information that we hold that you deem is no longer necessary or being processed unlawfully. We will respond to any requests for objection or erasure. We will act on each request based on its own merits. Portability There is a right to portability under the regulations. This means that you can request that we transfer any personal data that you have provided to us directly, under consent, so that it can be reused. Automated decision making and profiling You may request that no decisions are made by automated means using your personal data. This includes processing that reaches decisions that have a direct impact on you but has no human intervention, and profiling that analyses or aims to predict behaviour. We do not undertake any activities of this nature. How we keep information safe Technical controls We maintain technical controls across our infrastructure, networks and applications. These controls have a dual purpose; to stop any external access to the information we hold, and to monitor the legitimate access to the information from Electoral Commission employees. We hold a minimum amount of personal data in hard copy. Where it is necessary to hold hard copy information we keep it secure in locked filing cabinets or in a fireproof safe or PIN protected secure stores. All of our offices have card swipe security access controls in place. Organisational controls Our organisational controls ensure staff, contractors and other parties working on our behalf, protect personal data in line with our responsibilities under the regulations. These controls are actioned through our staffing and suppliers' contracts and our due diligence in relation to these. All our permanent, temporary and contract staff are subject to baseline security checks and are bound by our code of conduct which explicitly refers to adherence to our Data Protection Policy and Acceptable Use of E-communications and Facilities Policy. In our contracts with suppliers who process personal data on our behalf, we state exactly the activities that are covered by contract. Standard clauses in our terms and conditions adhere to the regulations. If something goes wrong (breaches) A breach refers to a circumstance that means the personal data we are processing is incorrectly destroyed, lost, altered, disclosed or accessed in an unauthorised way. In the event of a breach we will decide if it is necessary to notify the Information Commissioner's Office. We will base this decision on the likelihood of the breach negatively impacting on the individuals that the information relates to, taking into consideration any legal, financial and reputational damage. If we deem it necessary to notify the Information Commissioner's Office, then we will do this within 72 hours of identifying the breach, or as soon as possible. In exceptional circumstances where a breach is considered to present a high risk to the individuals' rights and freedoms, we will also notify those individuals of the breach. Public Records Act 1958 A very small number of records containing personal information are selected for permanent preservation at The National Archives. They are made available in accordance with the Freedom of Information Act 2000, as amended by the Data Protection Act 2018. Related content Freedom of Information Search our previous FOI responses, and find out how to make a request. Find out how to contact us Find our press releases, resources, and media contacts