

Information about the cyber-attack | Electoral Commission Search

Information about the cyber-attack You are in the Public notification of cyber-attack on Electoral Commission systems section Home Public notification of cyber-attack on Electoral Commission systems On this page About the cyber-attack About your data About voting and elections About our actions Contacting us First published: 8 August 2023 Last updated: 14 August 2023 What happened? The Electoral Commission has been the subject of a complex cyber-attack. The incident was identified in October 2022 after suspicious activity was detected on our systems. It became clear that hostile actors had first accessed the systems in August 2021. We worked with external security experts and the National Cyber Security Centre to investigate and secure our systems. About the cyber-attack What kind of information was accessible and how do I know if my data was accessed? How might the data be used? During the cyber-attack, our file sharing and email systems were accessible, which contain a broad range of information and data. The personal data most likely to have been accessible includes any names, addresses, email addresses, and any other personal data sent to us by email or held on the electoral registers. The following information is held by us and was accessible during the cyber-attack: The names and addresses of anyone in Great Britain who was registered to vote between 2014 and 2022, the names of those registered as overseas voters in the same period, and the names and addresses of anyone registered in Northern Ireland in 2018. The details of anonymous voters were not accessible, as we do not hold these. Any details provided to us via email or through forms on our website, such as the 'contact us online' form. The registers held by the Commission do not contain dates of birth, national insurance numbers, email addresses, information on your chosen voting method (post, proxy, or in person) or any other personal information. However, when people under 18 register to vote, the day and month they turn 18 is included on the register. This information could be used to calculate the date of birth for someone who is under 18. Information on people under 16 who are registered to vote in Scotland and Wales is not included in the registers held by the Commission. We know that data held by the Commission was accessible during the cyber-attack, but we have been unable to ascertain whether the attackers read or copied personal data held on our systems. We don't know how this data might be used, but according to our risk assessment (which was conducted in line with an ICO-recommended framework) the personal data held on electoral registers, typically name and address, does not in itself present a high risk to individuals. Further information is available in our Privacy Policy , and you can submit a form to access the information that we hold on you. How serious is this breach? We know it can be troubling to hear that your data may have been accessed. We regret that sufficient protections were not in place to prevent this cyber-attack and apologise to those affected. The data contained in the electoral registers is limited, and much of it is already in the public domain. According to the risk assessment used by the Information Commissioner's Office to assess the harm of data breaches, the personal data held on electoral registers, typically name and address, does not in itself present a high risk to individuals. It is possible however that this data could be combined with other data in the public domain, such as that which individuals choose to share themselves, to infer patterns of behaviour or to identify and profile individuals. Who was behind it? We do not know who is responsible for the attack. We reported the incident to the National Cyber Security Centre (NCSC). No groups or individuals have claimed responsibility for the attack. When and how did you find out? We were alerted to the attack by a suspicious pattern of log-in requests to our systems in October 2022. This led to an initial investigation and to the

identification of a possible breach. Following a thorough investigation, we were informed by our security partners that hostile actors had accessed our servers in August 2021. Who did you alert? We contacted the National Cyber Security Centre (NCSC) (which is a part of the Government Communication Headquarters (GCHQ)) and advised them that we suspected we were the victim of a successful cyber-attack. We worked with the NCSC and a security partner to secure our systems and investigate further. We reported the incident to the Information Commissioner's Office (ICO) within 72 hours of identifying the breach. Why are you informing the public now? There were several steps that we needed to take before we could make the incident public. We needed to remove the actors and their access to our system. We had to assess the extent of the incident to understand who might be impacted and liaise with the National Cyber Security Centre and the Information Commissioner's Office. We also needed to put additional security measures in place to prevent any similar attacks from taking place in the future. About your data Is there anything I need to do? Can I check if my details have been shared on the internet? There is no indication that information accessed during this cyber-attack has been published online, but there remains the possibility that some information has found its way into the public domain. There are a number of steps that can be taken to check whether your personal information is publicly available. If you have not opted out of the open electoral register, the information we hold will already be publicly accessible via websites like 192.com. If you want to check if your email address has been compromised, you can search <https://haveibeenpwned.com/> to see if your email address has been released through reported data breaches. If you think that you have supplied any financial data to us via email, there are free online credit check tools by reputable companies like Experian, which include online identity theft protection and monitoring. The National Cyber Security Centre has a suite of advice to help you and your family understand more about securing your data. For more detail, our Privacy Policy sets out the types of personal information that we collect, our legal basis for processing personal data and how to contact us if you have a question or concern. How can I check what information the Electoral Commission holds about me? To see what information we hold on you, you can submit a subject access request. The easiest way to do this is by submitting a form , but you can also make a subject access request by email or phone. When submitting a request, please let us know if you are asking for a search of the electoral register data, or all Commission systems, and what personal data you may have submitted to the Commission. In your request, please provide your name as it appears on the electoral register or your polling card, and a preferred contact email address for us to contact you about the request. We may follow up to ask you to provide proportionate information to confirm your identity, identify your data and process the request. Please note, if you are seeking the information of another adult or a child over the age of 13, you will need to demonstrate that you have the person's consent to collect their personal data and/or have legal authority to act on their behalf. Will someone be able to trace me to my home address? If you were registered to vote in Great Britain between 2014 and 2022, or in Northern Ireland in 2018, your address may have been accessed during this cyber-attack. The addresses of those registered as overseas voters were not accessible, nor were details of people registered anonymously which are not held by us. There is no indication that information accessed during this cyber-attack has been published online, but it is possible that individuals could be located if this information finds its way into the public domain. Please note, the addresses of those on the open register are already publicly available. The addresses of those who opt

out of the open register, are not made publicly available, but were accessible during this cyber-attack. If you want to check your registration status or opt-out of the open electoral register, please contact the electoral services team at your local authority. Their contact details can be found through the postcode search on our website. We know it can be troubling to hear that your data may have been accessed. We regret that sufficient protections were not in place to prevent this cyber-attack and apologise to those affected. Will this impact my credit score? No, this will not have an impact on your credit score. If you have any concerns about identity theft, you can contact Action Fraud , which is the national reporting centre for fraud and cybercrime in England, Wales and Northern Ireland, or Police Scotland , if you are based in Scotland. About voting and elections Will this have an impact on my ability to register to vote or take part in elections? No, this has no impact on your ability to take part in the democratic process and will not affect your current registration status or eligibility. The registers that we hold are copies that we use for research purposes and to check the permissibility of donors. Individual electoral registration officers for each local authority area hold the live versions of the electoral registers which are used to send out polling cards and at polling stations to check voters are registered and eligible to vote. The registers held by electoral registration officers are unaffected by this cyber-attack. Can someone impersonate me and vote? No, the data in this breach would not be enough for someone to impersonate you under current voting rules. What impact has the cyber-attack had on the security of UK elections? There has been no impact on the security of UK elections. The data accessed does not impact how people register, vote, or participate in democratic processes. It has no impact on the management of the electoral registers or on the running of elections. The UK's democratic process is significantly dispersed and key aspects of it remain based on paper documentation and counting. This means it would be very hard to use a cyber-attack to influence the process. Can you be sure the electoral registers were not edited or changed in anyway? We do not amend the copies of the electoral register that we hold in the performance of our work, and we are confident that the information within the files was not altered during the incident. The registers that we hold are copies that we use to check the permissibility of donations and for research purposes. Individual electoral registration officers for each local authority area manage the registration processes and hold the live versions of the electoral registers which are used to send out polling cards, and at polling stations to check voters are registered and eligible to vote. How can I opt out of the open register? There are two versions of the electoral register. The full version includes the name and address of everyone who is registered to vote, except those who register to vote anonymously. The open register is an extract of the full electoral register. This version is available to anyone who wants to buy it, such as businesses or charities. You can opt out of the open register when you register to vote. If you are already registered to vote and want to opt out, you can do so at any time, by contacting your local electoral registration officer . The request must contain your full name, and address, and you will need confirm that you want to be removed from the open/register. You can find contact details for your local electoral registration officer by entering your postcode into our search . About our actions What steps has the Commission taken to ensure its system are now secure? We have taken steps to secure our systems against future attacks and improved our protections around personal data. We have strengthened our network login requirements, improved the monitoring and alert system for active threats and reviewed and updated our firewall policies. We have worked with external security

experts and the National Cyber Security Centre to investigate and secure our systems.

Contacting us How do I contact the Commission to complain, ask a question about this incident or to request the information the Commission holds on me? In the first instance, please read the information available in our Public Notification . You can submit a form if you still have questions, or if you want to: make a Subject Access Request request erasure make a Freedom of Information request submit a complaint Submit a form Who else can I raise concerns with about this incident? We would encourage you to contact us in the first instance with any concerns or questions. If you are not happy with our handling of your questions or subject access requests, you can contact the Information Commissioner's Office, as the UK supervisory authority for data protection, via their online form.

Public notification of cyber-attack on Electoral Commission systems | Electoral Commission Search Public notification of cyber-attack on Electoral Commission systems You are in the section Home about the cyber-attack Information about the cyber-attack First published: 8 August 2023 Last updated: 8 August 2023 Introduction The Electoral Commission has a duty under Articles 33 and 34 of the UK General Data Protection Regulation to notify data subjects if their data has been breached by inappropriate access, loss, or theft from our systems. This notification gives important information about the personal data affected, the potential impact on individuals, and measures we've taken in response to a complex cyber-attack. The incident was identified in October 2022 after suspicious activity was detected on our systems. It became clear that hostile actors had first accessed the systems in August 2021. During the cyber-attack, the perpetrators had access to the Commission's servers which held our email, our control systems, and copies of the electoral registers. They were able to access reference copies of the electoral registers, held by the Commission for research purposes and to enable permissibility checks on political donations. The registers held at the time of the cyber-attack include the name and address of anyone in Great Britain who was registered to vote between 2014 and 2022, the names of those registered as overseas voters during the same period, and the names and addresses of anyone registered in Northern Ireland in 2018. The registers did not include the details of those registered anonymously. The Commission's email system was also accessible during the attack. We understand the concern this attack may cause and apologise to those affected. Since the attack was discovered, we have worked with security specialists to investigate the incident and have taken action to secure our systems and reduce the risk of future attacks. Public notification It is our assessment that the information affected by this breach does not pose a high risk to individuals and this notification is being given due to the high volume of personal data potentially viewed or removed during the cyber-attack. Personal data affected by this incident: Personal data contained in email system of the Commission: Name, first name and surname. Email addresses (personal and/or business). Home address if included in a webform or email. Contact telephone number (personal and/or business). Content of the webform and email that may contain personal data. Any personal images sent to the Commission. Personal data contained in Electoral Register entries: Name, first name and surname Home address in register entries Date on which a person achieves voting age that year. Electoral Register data not held by the Commission: Anonymous registrations Address of overseas electors registered outside of the UK. Electoral register copies The Commission holds copies of the electoral registers to enable its statutory functions. They are used for research purposes and to enable permissibility checks on political donations. The electoral register data held by the Commission has not been amended or changed in anyway as a result of the attack and remains in the form in which we received it. The data contained in the registers is limited, and much of it is already in the public domain. Our online privacy policy is accessible online via the following link <https://www.electoralcommission.org.uk/privacy-policy> Impact on individuals According to the risk assessment used by the Information Commissioner's Office to assess the harm of data breaches, the personal data held on the electoral registers – typically name and address – does not in itself present a high risk to individuals. It is possible however that this data could be combined with other data in the public domain, such as that which individuals choose to share themselves, to infer patterns of behaviour or to identify and profile individuals. The attack has not had an impact on the electoral process, has not affected the

rights or access to the democratic process of any individual, nor has it affected anyone's electoral registration status. The personal data held on the Commission's email servers is also unlikely to present a high risk to individuals unless someone has sent us sensitive or personal information in the body of an email, as an attachment or via a form on our website, such information may include medical conditions, gender, sexuality, or personal financial details. Information related to donations and/or loans to registered political parties and non-party campaigners is held in a system not affected by this incident. No immediate action needs to be taken in response to this notification. However, anyone who has been in contact with the Commission, or who was registered to vote in Great Britain between 2014 and 2022, and in Northern Ireland in 2018, should remain vigilant for unauthorised use or release of their personal data. If you have concerns over personal data which you may have sent to the Commission, please contact our Data Protection Officer, using the details below.

Mitigations We have taken steps to secure our systems against future attacks and improved our protections around personal data. We have strengthened our network login requirements, improved the monitoring and alert system for active threats and reviewed and updated our firewall policies. The Commission has worked with external security experts and the National Cyber Security Centre to investigate and secure its systems. Data subjects retain the right to complain to the UK Supervisory Authority, the Information Commissioner's Office (ICO). Contacting us about the cyber-attack

The Electoral Commission London office address 3 Bunhill Row, London EC1Y 8YZ, email: dataprotection@electoralcommission.org.uk for the purposes of this notification. The Data Protection officer is Andrew Simpson, Head of Digital, Data, Technology and Facilities. Information about the cyber-attack

Read answers to questions you may have about the cyber-attack

Submit our form to find out about your data, or to make a complaint

about the cyber-attack | Electoral Commission Search about
the cyber-attack You are in the Public notification of cyber-attack on Electoral
Commission systems section Home Public notification of cyber-attack on Electoral
Commission systems First published: 8 August 2023 Last updated: 8 August 2023 Summary
Before contacting us about the cyber-attack, please read the information available in
our Public Notification . You can submit a form if you want to: make a Subject Access
Request request erasure make a Freedom of Information request submit a complaint
About Subject Access Requests and erasure requests About Subject Access Requests and
erasure requests Subject Access Requests You have the right to ask us whether or not
we are using or storing your personal information. You can ask what personal
information we hold about you, how we're using it, who we're sharing it with, and
where we got your data from. You can also ask us for copies of your personal
information, verbally or in writing. When you submit a subject access request, you
will need to confirm if you want to find out about data on the electoral registers,
or about emails or forms on our website you submitted. Erasure requests Individuals
have the right to have personal data erased, which is also known as the 'right to be
forgotten'. The right only applies to data held at the time the request is received.
It does not apply to data that may be created in the future. The right is not
absolute and only applies in certain circumstances. When you submit an erasure
request, you will need to confirm if you want to find out about data on the electoral
registers, or about emails or forms on our website you submitted. Data protection
information request Data protection information request Your name Your email address
Your email address Confirm email address Select your reason for contacting us Make a
Subject Access Request Request erasure Make a Freedom of Information request Submit a
complaint Other Status message Make a Subject Access Request We are required under
data protection law to request proportionate information to ensure we are locating
your data and to confirm your identity. Select whether you're contacting us about
your data on the electoral registers, or about emails or forms on the website you
submitted Data on the electoral registers Emails or website forms Data on the
electoral registers, and emails or website forms Name Please provide your name as it
appeared on the electoral register between 2014 and 2022. Address Please provide the
address or addresses you were registered to vote at between 2014 and 2022. Email
address Please provide the email address that you used to contact us, or that you
entered into a form on our website. Date Please provide approximate dates of when you
contacted us by email, or when you submitted a form on our website. Details If you
can, please provide details of who you contacted (including their email address if
you have it), or the form on our website that you submitted. Information message
Request erasure We are required under data protection law to request proportionate
information to ensure we are locating your data and to confirm your identity. Select
whether you're contacting us about your data on the electoral registers, or about
emails or forms on the website you submitted Data on the electoral registers Emails
or website forms Data on the electoral registers, and emails or website forms Name
Please provide your name as it appeared on the electoral register between 2014 and
2022. Address Please provide the address or addresses you were registered to vote at
between 2014 and 2022. Email address Please provide the email address that you used
to contact us, or that you entered into a form on our website. Date Please provide
approximate dates of when you contacted us by email, or when you submitted a form on
our website. Details If you can, please provide details of who you contacted
(including their email address if you have it), or the form on our website that you
submitted. Information message Freedom of Information request We will respond to your

request using the email address you provided. If you would prefer a response in
hardcopy please let us know, and we will contact you to complete this aspect of your
request. Details Information message Submit a complaint We will respond to your
request using the email address you provided. If you would prefer a response in
hardcopy please let us know, and we will contact you to complete this aspect of your
request. Details of your complaint Details of your reason for contacting us Leave
this field blank

requires us to provide access to the process of elections for electoral observers, as individuals or on behalf of third party organisations, and representatives of the

Electoral Commission. We are required to create, administer, maintain and enforce the code of practice for electoral observers. We are also required to publish the code of

practice and to have regard to this published code of practice when exercising our

right to enforce the code. Please see our observer code of practice and application

form. What we collect name of applicant individual applicants home postal address for

receipt of badge telephone numbers for us to contact the applicant email address to

provide us to contact the applicant during the process and provide information as

required in advance of elections date of birth in relation to the statutory age

qualification for observers a digital photograph of the applicant, for use on an

identification badge a legible copy of supporting photo ID confirming your name and

age This information is collected only to ensure that we issue accreditation to the

requesting individual or individual representing an accredited organisation and is

laid out in the code of conduct for electoral observers. Political campaigning To

become an accredited electoral observer we will undertake searches of the internet

and social media to look for any evidence of political campaigning or political

activity that could compromise the impartiality of this role. We may also look for

information that indicates risk to the electoral event or individuals working to

deliver it. The requirement for us to undertake these checks on political neutrality

and risk to the event are included in the in the observer code of practice and

application form. These checks may result in information related to you being stored

in the electoral observer section of our document management system and may be shared

with the police. Technical controls We will retain your information in the electoral

observers section of our document management system. If you provide the documentation

in electronic form it will be retained as far as possible in the format in which you

sent it. Where you have provided hard copy versions of the documentation this will be

scanned in to PDF format and stored in our document management system. Images will be

stored in the document management system in JPEG format. The electoral observers area

of the document management system is managed with unique permission limited to staff

roles that administer and approve the process. The ICT and Information Management

team have permission to access this section only to provide technical support to the

process. Retention We will not retain your information for longer than is necessary.

The accreditation lasts until 31 December of the year in which you apply. We will

retain your information for the time that you are accredited with the scheme and for

one year after the accreditation has lapsed. After this time your information will be

disposed of securely and you will need to provide all information again. This applies

to applications submitted in hard copy and electronic format. Legal basis We have a

number of functions that are set out in the Political Parties, Elections and

Referendums Act 2000. These processes require us to collect and process personal

data. This is carried out under the legal basis that the processing is necessary for

the performance of our public task which is set out in UK law. For example, the

administration of applications to observe the electoral process as an individual, on

behalf of an organisation or as a representative of the Commission. Publishing We

maintain and publish three registers: accredited electoral observers accredited

organisations (XLS) authorised Commission representatives These are also available for public inspection at our offices on request. The published information is only for currently accredited observers and contains: electoral observer card ID number first name and surname type of accreditation organisation name if applicable date added to register valid from date valid to date Sharing We do not routinely share the information of electoral observers with third parties. We may be asked to share specific information with other bodies such as the police. Any request such as this will be considered on an individual basis and the rights of the data subject will be considered against any restrictions. Your rights Some rights, for example restriction and objection, may not be able to be met as this processing is part of our statutory function. We will only process the data for the purposes as defined in law. If additional processing is necessary to fulfil this statutory function, we shall take reasonable steps to inform you of this prior to the processing. If you object to the use of your personal data as described to support the electoral observers scheme, we will be unable to process your application. Related content What we do in elections about what we do in elections Find out how to contact us Find out about accessibility and our website

for a job You are in the section Home On this page Overview What information we collect Legal basis for collecting information How we use your information Retention of your information Your rights First published: 20 June 2019 Last updated: 2 August 2019 Overview If you are applying for a job with us you should do so via our online recruitment system. If you are applying for a job through a recruitment agency, you should refer to the agency's privacy notice to understand how your personal data will be processed. What information we collect and why We will collect personal information including your work history, contact details and declarations about past criminal convictions and political activity. We need this information so we can assess your application and contact you about it. Legal basis for collecting information We will ask for your consent for us to process this information when you register through our online recruitment system. How we use your information We will use the information you provide to assess your suitability for the role you have applied for. Our human resources team will have full access to this information. Hiring managers' shortlist of applications for interview will not include your name or contact details or your equal opportunities information if you have provided it. We might ask you to attend an interview and complete tests. Information will be generated by you and by us. For example, you might complete a written test or we might take interview notes. This information is held by us. Retention of your information For unsuccessful applicants, we will keep your information for six months from the closing date to apply for the role. For successful applicants, we will transfer your information to our internal systems and process it under the terms of our employment contract. Your rights When you provide information with your application you do so under consent and you may withdraw your consent for us to process this information at any time before entering into an employment contract with us. If you withdraw your consent for us to process your information this will mean we are unable to consider your application for the role. We will respond to any requests for access, rectification, erasure, restriction or objection about this information and act on each request based on its own merits. Related content What we do in elections about what we do in elections Find out how to contact us Find out about accessibility and our website

The Electoral Registers | Electoral Commission Search The Electoral Registers You are in the section Home On this page What we collect Legal basis for processing data Retention Sharing Your rights First published: 18 June 2019 Last updated: 8 August 2023 What we collect and why We collect copies of the full electoral register and updates to the register from Electoral Registration Officers (EROs) who are the primary controller of the Electoral Register in each Local Authority except Northern Ireland where the Electoral Office of Northern Ireland (EONI) performs that function for Northern Ireland. We also collect copies of extracts of Electoral Registers used in polling stations after elections which we refer to as marked register copies. To ensure safe transmission of this data between EROs and the Electoral Commission, we recommend the use of our secure cloud-based file transfer platform. This platform is secured with two factor authentication and its data is stored in UK based data centres. Once the registers arrive at the Electoral Commission, we load them into a secure electronic filing system which is only accessible by staff whose responsibilities include the functions set out below.

Legal basis for processing data Electoral Registration Officers (ERO) have a legal obligation to share the full electoral registers collected for Local Government Elections, UK Parliamentary Elections, and elections to the Scottish and Welsh Parliaments (referred to as the registers) with a number of organisations including the Electoral Commission. The supply of electoral registers to the Electoral Commission is to allow for the exercise of its statutory functions under the Political Parties Elections and Referendums Act 2000 (PPERA). We have two legal bases for processing electoral register data. For the full registers we process this information as part of our public task or in the exercise of our official authority under our statutory functions in the Political Parties, Elections and Referendums Act 2000 (PPERA). We collect and store the Register of Electors to perform our legal functions under PPERA, including by checking whether donations accepted, and transactions entered into by, registered political parties are permissible under the law and considering enforcement action under PPERA if they are not. For the copies of marked registers and copies of the full registers our legal basis for processing is as part of our public task under PPERA to undertake historical and statistical research in the public interest specifically to report, review and provide advice and assistance on elections and electoral matters such as voter registration processes and attitudes to registering to vote. Longitudinal research requires a longer retention period. Reports are published into the public domain via the Commission website and deposited with the appropriate legal deposit libraries.

Retention We retain copies of the full registers for five years which aligns with a typical full election cycle for each relevant election under PPERA this allows a reasonable time frame to check reports after the polls for compliance purposes and to allow for any actions under our enforcement role. Limited extracts may be retained in enforcement case materials for the retention period of the case. We retain copies of the marked registers from 2014 onwards for research purposes only.

Sharing The Electoral Commission does not routinely share electoral register data with other organisations. Electoral register data could be shared if requested by law enforcement agencies or UK Police Services. Each request from relevant authorities is assessed on a case-by-case basis. The Commission may transfer this data as part of an evidential disclosure to the Crown Prosecution Service (or devolved nations equivalent) as part of preparing for criminal action, or as part of information required for judicial proceedings, or legal proceedings. The Electoral Commission will share Electoral Register data with partner research academics and organisations under contract, such

as IPSOS Mori for the Survey of the Electoral Register and the British Election Survey, to support the understanding of and research into Electoral Registration. Your rights We will not be able to grant rights of erasure, rectification, or objection to data from the registers as we are not the primary data controller for Electoral Registers. You must ask the relevant Electoral Registration Officer or the EONI in Northern Ireland any questions about accuracy. We cannot meet any request to stop processing the data held in the registers if it concerns our statutory duty relating to permissibility checking or in data held for research purposes as a point in time record of the Register. Data subjects retain the right to complain to the UK Supervisory Authority, the Information Commissioner's Office (ICO). The Electoral Commission London office address: 3 Bunhill Row, London, EC1Y 8YZ Email: dataprotection@electoralcommission.org.uk for the purposes of this notification. The Data Protection officer is Andrew Simpson, Head of Digital, Data, Technology and Facilities. Related content Freedom of Information Search our previous FOI responses, and find out how to make a request. Find out how to contact us What we do in elections about what we do in elections

entities You are in the section Home On this page Legal basis for processing data What information we collect First published: 19 June 2019 Last updated: 19 June 2019 Legal basis for processing data Our regulatory functions are set out in the Political Parties, Elections and Referendums Act 2000. These functions require us to collect and process personal data. We do this under the legal basis that the processing is necessary for our public task which is set out in UK law. For example, maintaining a register of political parties across the UK and publishing donations and loans. Regulated entities include political parties, minor parties, non-party campaigners, permitted participants, regulated donees and unincorporated associations. What information we collect and why Registration of political parties and maintenance of the register of parties When registering, regulated entities need to provide us with some information about their organisation. What information the entity will need to provide depends on what type of entity they are and what type of application they are making. As an example, depending on the entity and the application, the information required may include but is not limited to: a financial scheme a constitution the names of the persons who will fill the roles required by the legislation and their address the names of other participators involved in the entity as required by the legislation the address of the entity We may also ask the regulated entity to provide further information in relation to their application as necessary to undertake our public task which is set out in UK law. Some entities may need to confirm their registered details annually, as well as keep us updated throughout the year with any changes to their registered details so that we can ensure that the information we hold, including person information, is accurate. This improves the accuracy of the register and meets your rights concerning rectification and in some cases erasure. We have a statutory duty to make certain registers of regulated entities available to the public and we do this by publishing those registers here. Financial returns Regulated entities must submit financial returns to us, including statement of accounts, party spending relating to elections and referendums and details of donations and loans. These returns will contain personal data about party or campaign officials, suppliers, lenders and donors. Financial returns may contain information that would reveal a Data Subject's political views and is therefore considered to be special category personal data. The condition for processing this type of data is that it is in the substantial public interest and has a basis in UK law under the Political Parties, Elections and Referendums Act 2000. We have a statutory duty to make financial return details available to the public and we do this by publishing information on our website. We encourage regulated entities to submit financial returns via our secure online system. We host this system on our network and control access to information via individual log in details. We also log changes to data within the system for audit purposes. Publishing details from regulated entities We publish details of registered entities' donations and loans, annual statement of accounts, campaign and referendum spending on our online database. Details include: names of people appointed to official roles names of donors party address name and address of suppliers for sole traders Sharing information from regulated entities We may share this information with our enforcement team to determine if we need to investigate a breach of political finance rules. Your rights We may not be able to meet some rights, for example restriction and objection, because this processing is part of our statutory function. We will only process the data for the purposes defined in the Political Parties, Elections and Referendums Act 2000 . Related content What we do in elections about what we do

in elections Find out how to contact us Find out about accessibility and our website

Election information and polling station finder | Electoral Commission Search
Election information and polling station finder You are in the section Home
First published: 27 April 2023 Last updated: 27 April 2023 Introduction We provide a year-round election lookup and polling station finder , delivered in partnership with Democracy Club Community Interest Company (Company number: 09461226). This tool helps people quickly find out which elections are taking place in their area, providing details of their polling station and local council addresses. The Electoral Commission and Democracy Club are the “data controllers” of your personal data. This means that the Electoral Commission and Democracy Club decide what your personal data is used for, and the ways in which it is processed. As data controllers, the Electoral Commission and Democracy Club have the responsibility to comply with, and to demonstrate compliance with, data protection law. We recommend referring to the Democracy Club’s privacy policy for more information on how they will process your personal data. We process personal data to support the delivery of our statutory functions, in particular the duty to promote public awareness of the electoral system under the Political Parties, Elections and Referendums Act 2000. Data we collect from users of the service Our election lookup and polling station finder provides information to users based on their postcode. This data is not retained by the Electoral Commission but is collected by Democracy Club. Postcodes are stored anonymously, to produce important statistics about usage of the service in different areas of the UK. This data helps the Electoral Commission and Democracy Club to improve the service we offer. We recommend referring to the Democracy Club’s privacy policy for more information on how they will process your personal data. Users of election information and polling station finders hosted on other sites We also make election information, polling station locations and local council addresses available to other organisations via our Electoral Commission API and lookup widget. When users access data via organisations using our API or lookup widget, the request to our API includes the user’s postcode. This data is not retained by the Electoral Commission but is collected by Democracy Club. Postcodes are stored anonymously, to produce important statistics about usage of the service in different areas of the UK. This data helps the Electoral Commission and Democracy to improve the service we offer. We recommend referring to the Democracy Club’s privacy policy for more information on how they will process your personal data. Cookies We only use necessary cookies on this website for the authentication of users. This is required for the operation of the website. For more information, please see our Cookie policy .

When we contact you | Electoral Commission Search When we contact you You are in the section Home On this page Overview How we use and store information First published: 18 June 2019 Last updated: 18 June 2019 Overview

We maintain contact details for individuals including elected representatives, electoral administrators, political parties, registered campaigners and others. We collect this information at the point of inbound contact or via publicly accessible data sources. How we use and store information We use this information to send newsletters and updates on important developments about electoral administration, electoral registration and political finance. This activity forms part of our public task which has its basis in the Political Parties, Elections and Referendums Act 2000. We store this information in a customer and contact management system and use network controls to ensure only members of staff that require access to this information have it. We monitor access through audit logs so that we can attribute any changes to the data we hold to a named member of staff. We audit this information annually to ensure accuracy and to deactivate redundant records. At this point we replace personal data from redundant records with artificial identifiers, to maintain a record of the contact but remove the personal data that is available to staff. We may store personal data with MailChimp to automate the way we send newsletters and audit the reach of this content. MailChimp is compliant with General Data Protection Regulation requirements and we retain control over the personal data stored on its platform. We will respond to any requests for access, rectification, erasure, restriction or objection about this data. We will act on each request based on its own merits.

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 goods 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

You are in the [section Home](#) [On this page](#) [Overview](#) [What information we collect](#) [Legal basis for collecting information](#) [Publishing information](#) [Sharing information](#) [Your rights](#) [First published: 20 June 2019](#) [Last updated: 20 June 2019](#) [Overview](#) [The Political Parties, Elections and Referendums Act 2000 \(PPERA\)](#) requires us to prepare and publish guidance as to the use of our powers to investigate and sanction potential offences and contraventions of PPERA. This enforcement policy fulfils that requirement. We are then required to have regard to this published guidance when exercising our enforcement functions. Please see our [enforcement policy](#) for more information. [What information we collect and why](#) In order to determine if an offence or contravention under PPERA has occurred, we may need to make enquiries of persons that we believe can provide relevant information. We will ask for documents, information and explanations on a voluntary basis or by using our investigatory powers, as appropriate. We may do this in writing or on the telephone, or by arranging meetings or statutory or voluntary interviews, depending on the circumstances. [Legal basis for collecting information](#) forms part of our public task as set out in PPERA. Some of the information we collect to support this work is classified as special category personal data. We process this for reason of substantial public interest, which has a basis in UK law. [Publishing information](#) Where there is a public interest to do so, we may make a media statement when an investigation starts or if there is a change to its scope. Once an investigation is concluded we will publish the outcome on our website. [Sharing information](#) We may share information about our investigations with: police and prosecutors in England and Wales, Scotland and Northern Ireland other regulators [Your rights](#) We may not be able to meet some rights, for example restriction and objection, because this processing is part of our statutory function. We will only process the data for the purposes as defined in PPERA. If additional processing is necessary to fulfil this statutory function, we shall take reasonable steps to inform you of this prior to the processing. [Related content](#) [What we do in elections](#) [about what we do in elections](#) [Find out how to contact us](#) [Find out about accessibility and our website](#)

When you contact us | Electoral Commission Search When you contact us You are in the section Home On this page Overview What we may record First published: 18 June 2019 Last updated: 18 June 2019 Overview You are able to contact us via our website, email, letter, telephone, Facebook or Twitter. We operate a public information line to support the public with queries about elections and the regulation of political finance. The legal basis for processing this information is that it is necessary for the performance of our public task as set out in law. What we may record When you contact us we may record the following information: name contact details social media handle location details of your query We will hold this information for one year from the last contact except where there is a regulatory reason for us to retain the information for longer. This may apply to contacts from political parties or electoral administrators. We may also use a UK-based external contact centre to manage calls and our social media accounts are managed via a third party tool. This service is operated under contracts that are compliant with General Data Protection Regulation and UK data protection legislation. This information is stored in a customer and contact management system and access to this information is via network controls which ensure that only members of staff that require access have it. This is monitored through audit logs so that we can attribute any changes to the data we hold to a named member of staff and the date of the change is recorded. Occasionally we may want to share the information you have given us with other organisations. For example, if you are raising an issue about electoral registration processes within a local authority area, we may want to speak to the Electoral Registration Officer at that local authority about this. In these circumstances, we will minimise the amount of personal data we share and focus on the general facts of your query. We will inform you of any such sharing as soon as possible. We will respond to any requests for access, rectification, erasure, restriction or objection about this information. Each request will be acted on based on its own merits. Related content Find out how to contact us Find out about accessibility and our website Find our press releases, resources, and media contacts

in the section Home On this page Cookies we use How to contact us General information First published: 20 June 2019 Last updated: 1 April 2022 Overview Cookies are files saved on your phone, tablet or computer when you visit a website. They are widely used to make websites work more efficiently. We use cookies to collect information about how you use our website, such as the pages you visit. We collect this information in a way that does not identify anyone. Cookies we use Analytics cookies We use Google Analytics to collect information about how visitors use our website. We use that information to help us improve the website for users. Google Analytics cookies store anonymous information about: How you got to the website, for example, using a search engine What pages you visit, and how long you spend on them What you click on the website Google Analytics collect cookies in a way that does not directly identify anyone. about how Google safeguard your data Name Expires Description _ga Two years These help us count how many people visit our website by tracking if you've visited before _gid 24 hours These help us count how many people visit our website by tracking if you've visited before _gat One minute These are used to throttle request rate This anonymous data is stored in Google Analytics and Google Tag Manager. It's accessed by our Digital Communications and Learning team to improve the performance of the website. You can opt out of being tracked by Google Analytics across all websites You can disable these cookies on our website at any time by updating your preferences Hotjar cookies We use Hotjar to better understand how you use our website. The service gives us information such as how much time users spend on a page, and what they choose to click on. We use this information to make improvements to the website for all users. We also use Hotjar to get feedback from users through surveys and polls. Hotjar uses cookies to collect information on users' behaviour and devices, such as: device's IP address (collected and stored anonymously) screen size device type browser geographic location (country only) preferred language Hotjar stores this information in a pseudonymised user profile. Neither Hotjar nor we will ever use this information to identify individual users or to match it with further data on an individual user. For more information, read Hotjar's privacy policy . You can disable these cookies on our website at any time by updating your preferences Name Expires Description _hjSessionUser_{site_id} One year Set when a user first lands on a page. It's used to persist the Hotjar User ID, unique to that site and to ensure data from subsequent visits to the same site are attributed to the same user ID. _hjClosedSurveyInvites One year Set once a user interacts with an External Link Survey invitation modal. It's used to make sure that the survey doesn't reappear if it's already been shown _hjDonePolls One year Set once a user completes a survey on the site. It's used to make sure that the survey doesn't reappear if it has already been completed _hjMinimizedPolls One year Set once a user minimises a poll on the site. It's used to make sure the poll stays minimised as a user navigates through the site _hjShownFeedbackMessage One year Set once a user minimises or completes Incoming Feedback. It's used to make sure Incoming Feedback stays minimised as a user navigates to other pages where it's set to show _hjid One year Set when a user first lands on a page with the Hotjar script. It's used to persist the Hotjar User ID, unique to that site on the browser. This ensures that behaviour in subsequent visits to the same site will be attributed to the same user ID _hjTLDTTest Session When the Hotjar script executes, it tries to determine the most generic cookie path it should use, instead of the page hostname. This is done so that cookies can be shared across subdomains (where applicable). To determine this, it tries to store the _hjTLDTTest cookie for different URL substring alternatives until

it fails. After this check, the cookie is removed

_hjUserAttributesHash Session User Attributes sent through the Hotjar Identify API are cached for the duration of the session in order to know when an attribute has changed and needs to be updated

_hjCachedUserAttributes Session This cookie stores User Attributes which are sent through the Hotjar Identify API, whenever the user is not in the sample. These attributes will only be saved if the user interacts with a Hotjar Feedback tool

_hjLocalStorageTest Under 100 ms This cookie is used to check if the Hotjar Tracking Script can use local storage. If it can, a value of 1 is set in this cookie. The data stored in **_hjLocalStorageTest** has no expiration time, but it is deleted almost immediately after it is created

_hjIncludedInPageviewSample 30 minutes Set to let Hotjar know whether that visitor is included in the data sampling defined by your site's pageview limit

_hjIncludedInSessionSample 30 minutes Set to let Hotjar know whether that visitor is included in the data sampling defined by your site's daily session limit

_hjAbsoluteSessionInProgress 30 minutes This cookie is used to detect the first pageview session of a user. This is a True/False flag set by the cookie

_hjFirstSeen Session This identifies a new user's first session. It's used by Recording filters to identify new user sessions.

_hjViewportId Session This is used to store user viewport details such as size and dimensions.

hjSession{site_id} 30 minutes This holds current session data. It is used to ensure subsequent requests in the session window are attributed to the same session.

_hjSessionTooLarge Session This causes Hotjar to stop collecting data if a session becomes too large. It is determined automatically by a signal from the WebSocket server if the session size exceeds the limit.

_hjSessionRejected Session This cookie, if present, set to '1' for the duration of a user's session, when Hotjar has rejected the session from connecting to our WebSocket due to server overload. It is applied in extremely rare situations to prevent severe performance issues.

_hjSessionResumed Session This is set when a session/recording is reconnected to Hotjar servers after a break in connection.

_hjRecordingEnabled Session Set when a Recording starts. It is used to read when the Recording module is initialized to see if the user is already in a recording in a particular session.

_hjRecordingLastActivity Session Set in Session storage as opposed to cookies. It's updated when a user recording starts and when data is sent through the WebSocket (the user performs an action that Hotjar records).

Performance cookies We may work with other partners to monitor and improve the performance of our website. These cookies measure things like how you view YouTube videos that are on our website. You can disable these cookies at any time by updating your preferences

Necessary cookies Necessary cookies make the website work. They do things like:

- Security settings** Remember which notifications you've seen so we don't show them again
- Remembers your cookie preferences** so that we don't have to ask you again

You may disable these cookies by changing your browser settings, but this may affect how the website functions.

Secure connection cookies Your browser uses cookies to make secure connections to websites with a 'https' URL. Different versions are used for different levels of security.

PEF online If you visit PEF Online, additional cookies to those set out above will be placed:

Name	Set by	Duration	Description
ASP.NET_SessionId	Website	Deleted when user leaves site or after 20 minutes of inactivity	Identifies user for duration of visit to website
PEFLanguage	Website	1 year	Identifies whether user prefers or Welsh language version of site

Search.electoralcommission.org.uk If you visit the political finance search site, no additional cookies to those set out above are used. This site only uses the Google Analytics cookies. Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, including how to see what cookies

have been set and how to manage and delete them, visit www.allaboutcookies.org To opt out of being tracked by Google Analytics across all websites visit <http://tools.google.com/dlpage/gaoptout> If you continue to access the Commission's websites without changing these settings, we will consider that you consent to the use of cookies as set out above. Please be aware that restricting cookies may impact on the functionality of our websites. How to contact us Queries about how we collect and handle personal information may be submitted to us by mail or email. Please send requests to: Andy Smith Data Protection Officer The Electoral Commission dataprotection@electoralcommission.org.uk General information This site has security measures in place to protect against the loss, misuse and alteration of material under our control. However, we accept no responsibility for alteration, manipulation or interpretation of its data once placed on the World Wide Web. Our information on the World Wide Web is subject to change without notice. Where we provide links to sites, we do not by doing so endorse any information or opinions appearing in them. We accept no liability over the availability of linked pages. This website is governed by UK law.

Electoral Commission API You are in the section Home First published: 20 August 2021 Last updated: 25 April 2023 Data we collect from users of the service We make election information, polling station locations and local council addresses available to other organisations via our Electoral Commission API and lookup widget. This service is delivered in partnership with Democracy Club Community Interest Company (Company number: 09461226). When users access election information via organisations using our API or lookup widget, the request to our API includes the user's postcode. The Electoral Commission and Democracy Club are the "data controllers" of this personal data. This means that the Electoral Commission and Democracy Club decide what this personal data is used for, and the ways in which it is processed. As data controllers, the Electoral Commission and Democracy Club have the responsibility to comply with, and to demonstrate compliance with, data protection law. We process personal data to support the delivery of our statutory functions, in particular the duty to promote public awareness of the electoral system under the Political Parties, Elections and Referendums Act 2000. Users' postcode data is not retained by the Electoral Commission but is collected by Democracy Club. Postcodes are stored anonymously, to produce important statistics about usage of the service in different areas of the UK. This data helps the Electoral Commission and Democracy Club to improve the service we offer. We recommend referring to the Democracy Club's privacy policy for more information on how they will process your personal data. Data we collect from API users When you register for an API key, we ask that you provide: Your name Your email address Name of company/organisation that you represent (where applicable) We will hold this information for as long as you are using the API key. When you are no longer using it, we will remove this information, unless we are required to hold on to this information by law. Cookies We only use necessary cookies on this website for the authentication of users. This is required for the operation of the website.