Data protection guidance for Electoral Registration Officers and Returning Officers
Data protection guidance for Electoral Registration Officers and Returning Officers
The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 apply to the processing of all personal data. Data protection legislation does not override requirements to gather and process information as set out in existing electoral law but there is impact on how this information is processed and the responsibilities of EROs and ROs to keep data subjects informed. You are personally responsible as an Electoral Registration Officer (ERO) and/or Returning Officer (RO) for ensuring that you comply with the requirements of current data protection legislation. This guidance, which includes practical examples where possible, is designed to support you in meeting: your duty to comply with the requirements of current data protection legislation your obligations, as they relate to your electoral administration responsibilities. It was developed in close consultation with colleagues across the electoral community including the Association of s (AEA), Department for Levelling Up, Housing & Communities (DLUHC), the Information Commissioner's Office (ICO), the Scottish Assessors Association (SAA) and the Society of Local Authority Chief Executives (SOLACE) to identify the impact of the legislation on EROs and ROs. 1 Book traversal links for Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller 1. In this resource we use 'RO' as a generic term to refer to all types of Returning Officer. ■ Back to content at footnote 1 Registering as a data controller You have a statutory duty to process certain personal data to maintain the electoral register and/or for the purpose of administering an election. As such, in line with current data protection legislation, you are acting as a data controller. Data controllers are required to register with the Information Commissioner's Office (ICO). 1 Advice from the ICO is that all data controllers will need to ensure that they are registered. This means that you must be registered separately to your council in your capacity as ERO and/or RO. The ICO have advised that if you are both an RO and an ERO one registration can cover both roles, and that where you have an additional role as a Regional RO, Police Area RO, Combined Authority RO etc, one registration can be used for all titles but this needs to be included in the name of the organisation when registering. In Scotland, where the ERO and the Assessor are the same person, the ICO have advised that one registration can also cover both roles, but both titles need to be included in the name of the organisation when registering. Registration fee The ICO have provided further guidance relating to the fee to register as a data controller on their website , including examples of how the fee should be calculated. When calculating the number of staff you employ, this should be determined pro rata, i.e. evened out throughout the year. For example, if you are an RO and you only employ staff in April and May to administer an election, the total staff employed in April and May would need to be apportioned throughout the year to determine the number of staff you employ. As such, it is likely that the fee would always fall into the lower category. If you are using a joint registration as ERO and RO, you will need to be careful when calculating the number of staff since you will need to consider the total staff across both functions. You should direct any questions in relation to registering as a data controller towards the ICO. 1. Digital Economy Act 2017 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Registering as a data controller Data protection guidance for Electoral Registration Officers and Returning Officers Accountability and transparency of data controllers Accountability and transparency of data controllers You must be able to demonstrate that you comply with your obligations as

a data controller, ensuring that personal data is processed lawfully, fairly and in a transparent manner. To achieve this, you should have and maintain written plans and records to provide an audit trail. You will have developed registration and election plans, and associated risk registers, that outline your processes and the safeguards that you have in place. You should keep these documents under review to ensure data protection remains integral and that they are compliant with current data protection legislation. Your plans and risk registers provide a sound basis for you to meet your obligations as a data processer. However, to show that you are processing personal data lawfully, fairly and in a transparent manner, you are also likely to need to implement further demonstrable processes. Data protection legislation impacts on your council as a whole, so you should not need to address the requirements in isolation. If you have not already done so, you should speak to your council's data protection or information officer. You should also utilise the ICO's website which has detailed guidance to support you in meeting your obligations, including specific guidance on accountability and transparency. Appointing a data protection officer A public authority must appoint a data protection officer (DPO) to advice on data protection issues. As ERO or RO, you are not currently included in the definition of a public authority contained in Schedule 1 to the Freedom of Information Act 2000 and are therefore not required to appoint a DPO for the conduct of your duties. However, you can choose to appoint a DPO if you wish. Your appointing council must have a DPO in place and you should liaise with them over good practice in relation to data protection. Last updated: 22 February 2023 Book traversal links for Accountability and transparency of data controllers Registering as a data controller Lawful basis for processing personal data Lawful basis for processing personal data For the processing of personal data to be lawful, it must be processed on a 'lawful basis'. 1 This includes: Legal obligation: the processing is necessary to comply with the law (not including contractual obligations); or Public task: the processing is necessary to perform a task in the public interest or in the exercise of official authority vested in you as the data controller; or Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks); or Consent: the individual has given clear consent for you to process their personal data for a specific purpose. For further information see the ICO's guidance on consent . Processing personal data without a lawful basis runs the risk of enforcement activity, including substantial fines, issued by the ICO, for further information see our guidance on data protection breaches and sanctions. The ICO have advised that in the main, the processing of personal data by EROs and ROs is likely to fall under the lawful basis that it is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller. It is for you to determine what the lawful basis for processing the data is, and to document your approach. You must clearly set out in your privacy notice which lawful basis you are relying on for processing and cite the relevant UK law where applicable. You may rely on more than one legal basis if you consider it appropriate. We have provided examples of lawful processing based on processing to perform a public task vested in you by UK law. You should undertake an audit of all the personal data that you collect to determine the lawful basis on which you are collecting/processing it. 1. Article 6 General Data Protection Regulation 2018 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Lawful basis for processing

personal data Accountability and transparency of data controllers Processing personal data for the performance of a public task Processing personal data for the performance of a public task This lawful basis for processing personal data covers: public functions and powers that are set out in UK law the performance of specific tasks in the public interest set out in UK law In the following situations, the lawful basis for the processing is the performance of a public task (i.e. maintaining the register of electors, and administering the election) in the public interest, as provided for in electoral law: An application to register to vote requires an ERO to process National Insurance numbers and dates of birth as part of the application. 1 Processing applications to register is part of the ERO's overall statutory duty to maintain the register of electors. 2 An RO is required to process personal data relating to a candidate for nomination purposes as part of the RO's overall statutory duty to administer the election in accordance with the rules. 3 You will also need to consider the appropriate lawful basis for the processing of personal data not covered by electoral legislation. For example, employment legislation may require you to process personal data relating to the right of polling station staff or canvassers to work in the UK. Where it is necessary for the performance of a public task to process personal data, you should determine and record what the basis for that public task is. This will enable you to demonstrate the lawful basis on which you are processing all personal data. The legislative references in the Commission's guidance for EROs and ROs may help with this. 1. Regulation 26 Representation of the People (England and Wales) Regulations 2001; Regulation 26 Representation of the People (Scotland) Regulations 2001 ■ Back to content at footnote 1 2. Section 9 Representation of the People Act 1983 (RPA) ■ Back to content at footnote 2 3. S23 RPA1983 ■ Back to content at footnote 3 Last updated: 22 February 2023 Book traversal links for Processing personal data for the performance of a public task Lawful basis for processing personal data Processing personal data and the edited register Processing personal data and the edited register As an ERO you are required to publish an edited register. 1 You are required to include electors details in the edited register if they do not opt out. The ICO have confirmed that as legislation provides for a statutory opt-out, coupled with the duties placed on EROs, this means that EROs are processing personal data for inclusion on the edited register is on the lawful basis that it that it is necessary to perform a public task. Therefore the data protection conditions for consent will not apply and will not impact on the edited register. 1. Regulation 93 Representation of the People (England and Wales) Regulations 2001; Regulation 93 Representation of the People (Scotland) Regulations 2001 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Processing personal data and the edited register Processing personal data for the performance of a public task Right to object to the processing of personal data Right to object to the processing of personal data Article 21 of the UK GDPR includes the right to object, meaning that the data subject can object to the processing of their personal data. This right does apply when processing is required for the performance of a public task (such as maintaining the electoral register). For example, legislation prevents an elector from changing their edited register preference on a canvass communication. 1 However, if you receive a response to a canvass communication and the elector has themselves clearly indicated on the form that they want to be removed from the open register until further notice, you should treat the canvass response as a notice under Article 21 of the UK GDPR and amend the register accordingly. Further information on this process is set out in our guidance for running electoral registration. The right to object to processing cannot however be

applied to information where the collection of or the nature of the processing is specified in electoral law. For example, the data subject can object to the processing of their email or telephone contact details in relation to electoral registration, but not to the use of their name or home address. You should maintain records to detail any request made under the right to object to processing to demonstrate that you are complying with the principles of processing personal data, ensuring that it is processed lawfully, fairly and in a transparent manner. Your Electoral Management Software (EMS) provider may have the facility to record consent against elector records and you should liaise with them to understand how to manage the process in practice. The email invitation to register (ITR) that you must use includes an unsubscribe option to allow electors to make a request under the right to object to the use of their contact information for this purpose. You should ensure that where you communicate with electors by email, you include an 'unsubscribe' option on all emails to allow the data subject to object to the use of their contact information for this purpose. 1. Regulation 93A Representation of the People (England and Wales) Regulations 2001; Regulation 93A Representation of the People (Scotland) Regulations 2001 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Right to object to the processing of personal data Processing personal data and the edited register Right to be forgotten Right to be forgotten Article 17 of the UK GDPR includes the right to be forgotten. This means that a data subject can request that you delete their information without undue delay. The right to be forgotten does not apply when: processing is required for the performance of a public task (such as the maintaining of electoral registers) it is necessary for archiving in the public interest For example, an elector cannot ask the ERO to remove them from old or historical electoral registers because their inclusion on that register was a result of a legal obligation on the ERO. However, an elector may request that information collected on grounds of consent (for example, where an elector gives consent to use of their email address) is deleted or removed at any time. The RO is required to publish notices relating to an election. These notices may include personal information relating to candidates, subscribers and agents. A person cannot use the right to be forgotten to require that their details are removed from a statutory notice. However, they could exercise the right to have their details removed from a notice you have published on your council website after the election, if the deadline for an election petition had passed (when the notice serves no further purpose). For this reason, once the petition deadline for an election has passed, you should either remove notices published on your website, or remove the personal data contained in these notices. You should also consider whether it is appropriate to retain that data. For example, if you have existing records of email addresses or phone numbers collected through an application to register, at the time that you next use that information, you should take appropriate measures such as: explaining the data subjects right to object to further processing linking to your privacy notice including the unsubscribe option, which allows the data subject to object to the use of their contact information for this purpose For more information see our guidance on document retention . Last updated: 22 February 2023 Book traversal links for Right to be forgotten Right to object to the processing of personal data Special categories of personal data Special categories of personal data Electoral legislation requires an individual applying to register to vote to provide their nationality or nationalities, or, if they are not able to provide that information, the reason they are not able to do so. 1 As ERO you are required to process this nationality data in order to determine which elections the elector is

entitled to vote at. Data protection legislation does not affect the requirement for nationality information to be provided, however, nationality data is classed as a special category of personal data because it may reveal an individual's racial or ethnic origin. You may also deal with special categories of personal data through: documents received as part of the documentary exceptions process documents received as part of an application for anonymous registration information relating to staff appointments Processing special category data Data protection legislation prohibits the processing of special categories of personal data unless an additional lawful basis beyond those for the main purposes of processing data is met. For electoral purposes, the appropriate lawful basis for processing special categories of personal data would be that it is necessary for reasons of substantial public interest and with a basis in UK law. For more information on this see our guidance on Lawful basis for processing personal data . To process nationality data you must have in place a policy document which must explain: the procedures for complying with the data protection principles the policies for retention and erasure Your policy document will need to reflect your: local processing procedures policies for the retention of personal data policies for the erasure of personal data This policy document must: be kept until six months after the processing ceases be reviewed and updated at appropriate times be made available to the ICO on request 1. Regulation 26 Representation of the People (England and Wales) Regulations 2001; Regulation 26 Representation of the People (Scotland) Regulations 2001 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Special categories of personal data Right to be forgotten Data protection impact assessments (DPIAs) Data protection impact assessments (DPIAs) Data protection impact assessments ensure that data protection principles are integral to the design of processes by helping to identify, assess and mitigate risks. Data protection legislation requires that a DPIA is undertaken before processing when: you are using new data processing technologies for example, if you introduce a new initiative to issue canvassers with tablets, you need to undertake a DPIA first. the processing is likely to result in a high risk to the rights and freedoms of individuals for example, processing applications for anonymous registration is high risk processing (see our guidance on high risk processing for further information). A DPIA is not required where a processing operation has a lawful basis that regulates the processing and a DPIA has already been undertaken. For example, if your canvassers are already using tablets and processing is underway you are not required to conduct a retrospective DPIA. However, you should ensure that data protection principles are integral to your existing processing operations, and a DPIA can help evidence this. When you undertake any new process, you should undertake DPIAs as a matter of good practice. This will enable you to demonstrate that data protection is integral to your processes and support the principle of accountability. We have produced the following template DPIA which is used by the Electoral Commission. Example Data Protection Impact Assessment (DPIA) (DOC) The template relates to our activities, so you will need to adapt it to make it relevant, but it may support you in undertaking your own DPIAs. You should speak to your council's Data Protection Officer/Information Officer before undertaking a DPIA. DPIAs and anonymous registration applications Applications for anonymous registration contain data relating to anonymous electors' or applicants' personal safety. The lawful basis for processing this data is set out in legislation but the processing is high risk due to the nature of the data. You should have a DPIA in place for processing anonymous registration applications, and if you don't you should undertake one. Last updated: 22 February 2023 Book traversal links for Data protection impact

assessments (DPIAs) Special categories of personal data Requirements of a Data Protection Impact Assessment (DPIA) Requirements of a Data Protection Impact Assessment (DPIA) Data protection legislation does not specify a particular process to be followed when undertaking a DPIA. However, it does set out minimum required features: a description of the proposed processing and the purposes – in relation to anonymous registration, this should include: what the personal data is who will have access how it will be stored who it will be disclosed to an assessment of the necessity and proportionality of the processing – in most cases for an ERO or RO this will be processing for the performance of a public task an assessment of the risks to the rights of the individuals affected the measures envisaged to address the risks and demonstrate compliance with data protection rules for example, the measures you put in place to keep the identity of anonymous electors secure A single DPIA may be undertaken where a set of similar processing operations present similar high risks. The ICO has provided guidance on DPIAs on their website which includes examples of good practice. You should: keep any DPIAs you have in place under review to determine if your processing operations require any further DPIA to be undertaken consider how you can ensure data protection is integral to all of your processing ensure that all your training – whether for canvassers, polling station staff, or your electoral services team – reflect data protection requirements. This will help you to embed the data protection principles in your work and demonstrate compliance ensure you discuss any data protection training with your council's Data Protection Officer/Information Officer Last updated: 22 February 2023 Book traversal links for Requirements of a Data Protection Impact Assessment (DPIA) Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Privacy notices - the right to be informed Data subjects must be provided with sufficient information to enable them to understand how their personal data is used. This is achieved via a privacy notice which is sometimes called a fair processing notice. You will need to ensure you have a privacy notice published on your website. This can be a standalone privacy notice or can be included as part of your council's privacy notice. The information in a privacy notice must be provided in clear plain language, particularly when addressed to a child, and be provided free of charge. It is important that your privacy notice is specific to your local circumstances and the personal data that you process. It must be kept up to date to meet any changes in your approach to processing data. Your council's data protection/information officer will be able to help you with the contents of the required notices. Due to the differences across ERO and RO functions due to devolution, shared services, differences in EMS suppliers and internal structures and processes within each council it is not appropriate for the Commission to provide a template privacy notice. In particular, your privacy notice needs to set out how you will use the personal data that is collected. The following bullet points are not an exhaustive list, but give an indication of the sort of things that could be covered in your privacy notice: the fact that personal data contained in the electoral register will be used to conduct an annual canvass, including issuing canvass communications to all households and following up with non-responding properties how information in the electoral register may be used using the prescribed wording to describe the electoral register and the open or edited register (as included on the voter registration form) the fact that personal data contained in the electoral register and absent voting lists will be used to issue poll cards in advance of an election that a postal voter's signature (where required) and date of birth provided on a postal voting statement will be compared against that postal voter's signature and date of birth held on the personal identifiers record You must

be clear for what purpose you collect, hold and use people's data – and ensure that you are not using it for other unrelated purposes. You should periodically review your privacy notices with your council's data protection officer/information officer to ensure they remain compliant with the current data protection legislation. You should ensure your privacy notice is clearly visible on your website and is referenced when communicating with electors and others. We have produced a checklist for what a privacy notice must contain: Checklist for Privacy Notice (DOC) Last updated: 22 February 2023 Book traversal links for Privacy notices - the right to be informed Requirements of a Data Protection Impact Assessment (DPIA) Notifying data subjects about how their personal data is used Notifying data subjects about how their personal data is used Data protection legislation sets out requirements for notifying data subjects about how their personal data is used. When data is collected directly from the data subject, the notice must be given at the point of collection. For example, a notice needs to be included: in letters requesting documentary evidence under the exceptions process on application forms for the appointment of election staff When data is not collected directly, the notice must be given to the data subject within one month or at the first point of contact. But this is not necessary if the data subject was notified of the terms of the privacy notice when the data was originally collected by the primary data controller (for example, if you use personal data collected by council tax to verify an applicant for registration, a notice is not required if one was given to the applicant by the council tax department when the personal data was originally collected). It is not necessary to provide a link to a privacy notice on poll cards. Poll cards do not collect personal information, they contain information from the electoral register and absent vote lists which are publicly available under electoral law. Your privacy notice should set out that personal data contained in the electoral register and absent voting lists will be used to issue poll cards in advance of an election. Last updated: 22 February 2023 Book traversal links for Notifying data subjects about how their personal data is used Privacy notices - the right to be informed Data protection considerations for the inspection of the electoral register Data protection considerations for the inspection of the electoral register We have produced a cover sheet for the inspection of the register which sets out how it may be used and the penalty for misuse. Cover sheet for copies of full register for inspection (DOC) You should maintain records of every person or organisation supplied with the electoral register and absent voting lists, not just those who pay to receive it. You should ensure that every person/organisation receiving the register, whether on publication, by sale, or on request, is aware that: they must only use the register for the purpose(s) specified in the Regulations permitting its supply once the purpose for which the register has been supplied has expired, they must securely destroy the register they understand penalty for misuse of the register We have included the information suggested above in the following cover sheets for the sale and supply on request of the electoral register: Cover sheet for copies of full register for sale (DOC) Cover sheet for copies of full register supplied free of charge on request (DOC) Last updated: 22 February 2023 Book traversal links for Data protection considerations for the inspection of the electoral register Notifying data subjects about how their personal data is used Inspecting council records as ERO Inspecting council records as ERO As ERO, you will need to demonstrate that all information obtained from inspecting council records or disclosed by your council complies with the principles of processing personal data, ensuring that it is processed lawfully, fairly and in a transparent manner. Maintaining records will help you to demonstrate

that you are complying with your obligations under data protection and electoral legislation. 1 You should keep a record of: the records to be checked a schedule of when those checks are carried out the lawful basis on which you are processing that information. 2 For example, your obligation as ERO to inspect records you are permitted to inspect as part of your duty to maintain the electoral register measures to ensure appropriate security are in place to protect the data, for example: encrypting or password protecting data whenever it is transmitted using secure storage the action you have taken on the basis of the information you have obtained retention and secure disposal of data in accordance with your document retention plan You should ensure you maintain records of the council records you inspect, and should have the maintenance of records as a clear part of your overall registration plan. Further guidance on inspecting council records 3 is contained in our guidance for EROs . 1. Regulation 35 and 35A Representation of the People (England and Wales) Regulations 2001 (RPR (E&W) 2001); Regulation 35 and 35A Representation of the People (Scotland) Regulations 2001 (RPR (S) 2001) ■ Back to content at footnote 1 2. Section 9A of the Representation of the People Act 1983 (RPA 1983) provides the statutory basis by which you process personal data obtained through council records ■ Back to content at footnote 2 3. Regulation 35 and 35A RPR (E&W) 2001; Regulation 35 and 35A RPR (S) 2001 ■ Back to content at footnote 3 Last updated: 20 March 2023 Book traversal links for Inspecting council records as ERO Data protection considerations for the inspection of the electoral register Document retention Document retention Personal data processed for any purpose must not be kept for longer than is necessary for that purpose. Once the purpose for collecting the data has passed, you need to consider if there is a reason for you to retain that data. Data protection legislation does permit personal data to be stored for longer periods if, subject to the implementation of appropriate safeguards, the data will be processed solely for: archiving purposes in the public interest scientific purposes historical purposes statistical purposes Examples might include old electoral registers held to determine the eligibility of overseas applicants, or election results. You should practice data minimisation – don't ask for, and process, personal data if you don't need it. For every document you possess, ask yourself "for what reason am I keeping this document?" Last updated: 22 February 2023 Book traversal links for Document retention Inspecting council records as ERO Document retention policy Document retention policy Maintaining your document retention policy will help you to: demonstrate that you are complying with the principles of processing personal data ensure that data is processed lawfully, fairly and in a transparent manner Your document retention policy should set out the following for all documents you receive and hold: whether the document contains personal data the lawful basis on which any personal data was collected your retention period your rationale for the retention period (which might relate to a requirement in electoral law, for example, home address forms at UK Parliamentary elections must be destroyed after 21 days) In some cases, maintaining your document retention policy will be straightforward as electoral legislation will require a set period for which documents are retained. For example, at a UK Parliamentary election, specific documents relating to the election must be retained for one year 1 and then, unless otherwise directed, be destroyed. In other cases, you will need to make a local decision and justify this in your document retention policy. If you are an ERO, your document retention policy will include (but will not be limited to) how you process and store documents received due to: an application to register (i.e. application form and any documentary evidence where required) an application for an absent vote your inspection of council records or your power to

require information from any other person for the purposes of maintaining the register a request to an applicant/elector for further information to help you determine if they are resident your power to require evidence as to age or nationality For further information, refer to the relevant section on Access and Supply in our guidance for EROs. Our guidance for ROs for each election type contains specific advice on the retention of election documents . Your retention plan should reflect your approach to the retention of all documents. For example, storage and retention of nomination papers and home address forms may differ for each election type. You will also need to consider your document retention policy for: notices published for the election staff records, including appointment and payment records 1. Rule 57, Schedule 1 Representation of the People Act 1983 ■ Back to content at footnote 1 Last updated: 20 March 2023 Book traversal links for Document retention policy Document retention Retention of election notices published on your website Retention of election notices published on your website You will need to ensure that election notices published on your website are removed at the appropriate time. Election notices serve specific purposes: for example, a statement of the candidates standing at an election. Once the election is over, and the opportunity to question that election has passed, the election notices have no further purpose. You will need to consider whether it is appropriate or necessary for election notices to remain published on your website beyond the expiry of the petition period for that election. Once the petition deadline for that election has passed, you should either remove notices published on your website, or remove the personal data contained in these notices. Unless there is a reason not to, for example a legal challenge, it is essential that you securely destroy documents in accordance with your document retention policy. You should appropriately label documents and tag electronic files with destruction dates. You should reference these dates in your electoral registration and election plans. You should ensure that you and your staff are familiar with and adhere to your document retention policy, and that it is up-to-date and covers every document you process. Last updated: 22 February 2023 Book traversal links for Retention of election notices published on your website Document retention policy Data storage Data storage As data controller, you have a duty to protect against unauthorised or unlawful processing and against accidental loss and are required to have appropriate technical and organisational measures in place to ensure a level of security, appropriate to the risk. 1 You must determine what appropriate security measures are in place to protect personal data. For example ensuring that personal data is encrypted when it is being transferred, thus ensuring that you act as a guardian for that data. Your council will have corporate standards and processes for data handling and security. Your Data Protection Officer will be able to advise you on the processes you use as part of carrying out your specific duties as RO and/or ERO. They will also be able to help you identify any risks to the security of the data you hold, whether on paper or stored electronically on your systems. You should ensure that you have processes in place to retrieve data and securely destroy it at the appropriate time, in accordance with your document retention policy. 1. Article 32 General Data Protection Regulation 2018 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Data storage Retention of election notices published on your website Using contractors and suppliers Using contractors and suppliers As a data controller, you may use a processor to act on your behalf to process data. For example, you are using a processor if you send register data to a contractor to provide an automated response facility during the canvass or send absent vote data to a contractor to produce postal ballot packs for

an election. Last updated: 22 February 2023 Book traversal links for Using contractors and suppliers Data storage Requirement for a written contract with a processor Requirement for a written contract with a processor Data protection legislation requires that whenever you use a processor, you must formalise the working relationship in a written contract which sets out: the subject matter, nature and purpose of the processing the obligations and rights of the data controller duration of the processing and the types of personal data and categories of data subjects The contract must also set out specific obligations on the processor, including that they: comply with your instructions are subject to a duty of confidentiality keep personal data secure and notify you of any breach maintain written records of the processing activities they carry out for you only use a sub-processor with your consent submit to audits and inspections and provide you with whatever information you need to ensure compliance with current data protection legislation delete or return all personal data to you as requested at the end of the contract As data controller, you are ultimately responsible for ensuring that personal data is processed in accordance with data protection principles. However, if a processor fails to meet any of its obligations, or acts against your instructions, then it may also be liable to pay damages or be subject to fines or other penalties or corrective measures. You should consider the guidance the ICO provides on ‘ Contracts and liabilities between controllers and processors ’ in relation to your contracts with data processors. Appointing data processors Data protection legislation requires that you only appoint a processor that can provide sufficient guarantees that the requirements of the current data protection legislation will be met. You should ensure that data protection is integral in any tender exercise (documenting your decision-making process) and that the requirements set out in our guidance are met in any contract awarded. You should also ensure that your existing contractors or suppliers are aware of their obligations under the current data protection legislation, and that any existing contracts meet the requirements set out in our guidance. Last updated: 22 February 2023 Book traversal links for Requirement for a written contract with a processor Using contractors and suppliers Data sharing agreements with external organisations Data sharing agreements with external organisations As ERO, you may be obtaining personal data from external partners. For example, you may receive student data from local higher education providers or receive data from care homes regarding their residents. In this situation, the external partner will be a data controller in their own right. It is strongly recommended that you agree a data sharing agreement or protocol with any external partners and have a written agreement when sharing data between data controllers, even though the legislation does not specifically require it. A written agreement or protocol will help both you and the external partner demonstrate that you are acting in accordance with the data protection principles and will help to avoid any liability implications of one party being seen as a controller and the other being seen as a processor. We have produced the following checklist that you can use when developing a data sharing agreement: Checklist for data sharing agreement (DOC) Alternatively, your council may have developed a template agreement that you can use. In any case, you should discuss any data sharing agreement with your council’s Data Protection Officer or Information Officer. Last updated: 22 February 2023 Book traversal links for Data sharing agreements with external organisations Requirement for a written contract with a processor Data sharing agreements and supply of the electoral register Data sharing agreements and supply of the electoral register Electoral law provides a statutory framework for the supply of the electoral register

and, as ERO, you must supply the register in accordance with the relevant regulations. 1 The recipient of the electoral register must only use the register for the purposes specified in those Regulations. 2 As ERO you could choose to have a data sharing agreement with an organisation relating to the supply of the register, a credit reference agency for example. However, there is no requirement for such an organisation to have an agreement with you. If you choose to have an agreement you would need to be careful that the provisions contained in it do not go beyond the requirements in the Regulations. You should ensure that you have written data-sharing agreements in place with external organisations where you are receiving/sharing data on an ongoing basis. We have produced the following checklist you can use to help you with this. Checklist for data sharing agreement (DOC) For EROs in Scotland, the Scottish Assessors Association (SAA) have made available the following data sharing agreement being used by EROs to share data in Scotland. Sharing good practice: Data sharing agreement – an example data sharing agreement 1. Representation of the People (England and Wales) Regulations 2001 (RPR(E&W)); Representation of the People (Scotland) Regulations 2001 (RPR(S)) ■ Back to content at footnote 1 2. RPR (E&W) 2001; RPR (S) 2001 ■ Back to content at footnote 2 Last updated: 22 February 2023 Book traversal links for Data sharing agreements and supply of the electoral register Data sharing agreements with external organisations Subject access requests Subject access requests A data subject is entitled to see personal information that is held about them. You must provide information requested by data subjects without delay and in any event within one month (although it can be extended to two months in certain conditions). There is no requirement for the request for a subject access request to be made in writing. You must be satisfied of the requester's identity before fulfilling the request. Subject to a few conditions, these must be provided free of charge. Subsequent copies of subject access requests may be charged for, but the charge must be reasonable and based on administrative costs. Providing Certificates of registration Under data protection legislation no charge can be made for fulfilling a subject access request unless the request can be deemed excessive or repetitive. In the majority of instances, providing confirmation of a data subject's entry on the register via a certificate of registration will not meet this test and therefore no charge should be made. Last updated: 22 February 2023 Book traversal links for Subject access requests Data sharing agreements and supply of the electoral register Access requests relating to crime prevention Access requests relating to crime prevention Data protection legislation provides an exemption to data processing rules for the purposes of crime prevention. 1 Where you receive a request for information that you hold you will therefore need to consider: the person or organisation making the request, the purpose of the request, and the enactment quoted requesting access If you are satisfied that the request is for the purposes of: the prevention or detection of crime, or the apprehension or prosecution of offenders then you should supply the data. The ERO must supply the full register to the council that appointed them. 2 An employee or councillor of that council may, disclose or make use of information contained in in the full register, where necessary for the discharge of a statutory function of the council relating to security, law enforcement and crime prevention (or, in England and Wales, any other local authority). If a request relates to the council's copy of the register, you should direct the request to your council's Monitoring Officer. 1. Schedule 2 Data Protection Act 2018 ■ Back to content at footnote 1 2. Regulation 107 Representation of the People (England and Wales) Regulations 2001; Regulation 106 Representation of the People (Scotland) Regulations 2001 ■ Back to content at footnote 2 Last updated:

22 February 2023 Book traversal links for Access requests relating to crime prevention Subject access requests Data protection breaches and sanctions Data protection breaches and sanctions You should ensure that your registration and election plans and risk registers highlight the safeguards you have in place to avoid a personal data breach, particularly when you are undertaking high risk activities – such as producing poll cards and postal votes. Last updated: 22 February 2023 Book traversal links for Data protection breaches and sanctions Access requests relating to crime prevention Personal data breaches Personal data breaches A personal data breach includes breaches that are the result of both accidental and deliberate causes. They may include: access by an unauthorised third party – for example, your EMS system/council network being hacked deliberate or accidental action (or inaction) by a controller or processor – for example, your print supplier failing to process all absent vote data you have sent them, meaning that some electors are disenfranchised because they do not receive their postal votes in time sending personal data to an incorrect recipient – for example, sending an electoral register to someone who is not entitled to receive it computing devices containing personal data being lost or stolen – for example, laptops or iPads containing register or election data being stolen alteration of personal data without permission – for example, a canvasser falsifying canvass responses You should have robust quality assurance and proof-checking processes in place to help detect any errors and avoid data breaches before they occur. For example, when producing postal votes, you should have in place a process for checking live proofs, including those for postal proxies. You should attend the issue of postal votes to check the actual stationery being produced. This will highlight if any of the signed-off proofs have been inadvertently altered. Once postal votes have been issued, you should monitor returns to ensure that you have received completed postal votes back from every polling district. This will help you identify at an early stage if the issue was incomplete. We have published guidance containing full details of the quality assurance measures you should have in place. Quality Assurance Guidance for ROs (PDF) Last updated: 22 February 2023 Book traversal links for Personal data breaches Data protection breaches and sanctions Requirement to notify when a personal data breach has occurred Requirement to notify when a personal data breach has occurred When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people’s rights and freedoms: if there is a risk, you must notify the ICO within 72 hours of becoming aware of the breach if there is a high risk – in addition to notifying the ICO, you must inform the individuals concerned directly without undue delay ICO guidance defines a high risk in terms of the severity of the potential or actual impact on individuals: “If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.” Where the risk is unlikely to impact on people’s rights and freedoms, you don’t have to report it to the ICO. If the risk is not high, you do not have to notify the individuals concerned. In both cases, you need to be able to justify your decision, so you should document your reasoning in line with the accountability principle. The ICO also has the power to compel you to inform affected individuals if they consider that there is a high risk. Last updated: 22 February 2023 Book traversal links for Requirement to notify when a personal data breach has occurred Personal data breaches Sanctions and penalties for

data breaches Sanctions and penalties for data breaches Under data protection legislation, fines of up to around £17.5 million or 4% of turnover (whichever is greater) may be imposed for: failure to process personal data on a lawful basis, infringing the rights of data subjects; failure by a data controller in relation to the engagement of processors; or failure of a processor to process data only in accordance with the controller's instructions; A maximum of £8.7million (or 2% annual turnover) applies for other breaches including: failure to maintain security of personal data failure to report breaches (including to the data subject where required) failure to maintain records of processing activities failure to undertake a Data Protection Impact Assessment when required to do so In addition to imposing fines, the ICO may audit offenders, issue reprimands and impose restrictions on the breaching party. Reputational damage could also be significant. You should make sure you understand the consequences of failing to comply with your data protection obligations, and ensure you have procedures in place to detect, report and investigate any personal data breach. Last updated: 22 February 2023 Book traversal links for Sanctions and penalties for data breaches Requirement to notify when a personal data breach has occurred Resources for Electoral Registration Officers and Returning Officers - Data protection Resources for Electoral Registration Officers and Returning Officers - Data protection Checklist for data sharing agreement (DOC) Checklist for Privacy Notice (DOC) Cover sheet for copies of full register for inspection (DOC) Cover sheet for copies of full register for sale (DOC) Cover sheet for copies of full register supplied free of charge on request (DOC) Example Data Protection Impact Assessment (DPIA) (DOC) Quality Assurance Guidance for ROs (PDF) Sharing good practice: Data sharing agreement – an example data sharing agreement Last updated: 22 February 2023 Book traversal links for Resources for Electoral Registration Officers and Returning Officers - Data protection Sanctions and penalties for data breaches