East Staffordshire Borough Council

INDIVIDUAL ELECTORAL REGISTRATION

PRIVACY IMPACT ASSESSMENT

Background

Data collection, sharing and processing must be undertaken within a clear legal framework with minimum intrusion on an individual's privacy. A Privacy Impact Assessment (PIA) can assess privacy risks to individuals as part of the collection, use and disclosure of information, within projects and policies that involve the processing of personal data.

This Privacy Impact Assessment (PIA) describes how data protection and privacy issues relating to Individual Electoral Registration may be identified, addressed and mitigated. The PIA must comply with the Data Protection Act (DPA) and any other relevant legislation. The benefits of the PIA are:

- The identification and management of risk;
- Avoidance of unnecessary costs;
- Prevention of inadequate solutions;
- Avoiding loss of trust and reputation;
- Informing citizens and partners of the organisation's communications strategy;
- Meeting and exceeding legal requirements.

This Privacy Impact Assessment is intended to be a living document and it may be updated to reflect further developments in the Individual Electoral Registration processes. Previous PIAs can be obtained from East Staffordshire Borough Council.

Individual Electoral Registration

The Electoral Registration and Administration Act 2013 introduces a major change to the electoral registration system by introducing Individual Electoral Registration (IER) in Great Britain in order to modernise the electoral registration system and tackle fraud. IER will replace the existing system of household registration from 10th June 2014 in England and Wales and from 19th September 2014 in Scotland. Electors will be asked to register individually and will be required to provide identifying information which will be checked ("verified") before the individual can be added to the electoral register. This process will replace the existing system of household registration.

It is expected that the majority of current electors will be transferred to the individual electoral register automatically via "confirmation" (matching electoral registers against records held by the Department for Work and Pensions). Therefore it will be

possible to confirm the majority of people on the existing electoral register at the transition to IER, without the need for them to apply individually and they will not be required to share their personal data in order to remain on the electoral register when IER is introduced.

Verification of existing electors who do not match with DWP's database during the confirmation exercise, and verification of new applications will involve the handling of personal data in a new way. Individuals applying to register to vote will be required to provide additional information which will be used to verify their application before they are added to the electoral register. With approximately 46 million people currently on the electoral registers in Great Britain this change affects a large proportion of the population.

Reducing Fraud

While electoral fraud is rare, any fraud undermines public confidence. Therefore the Coalition Government agreed to speed up the introduction of individual registration to improve security.

There remain a significant number of people who perceive fraud to be a problem (34% per cent of people surveyed for the Electoral Commission's Winter Research 2013) and this can have a corrosive effect on trust in our political system.

IER will improve confidence in the system of electoral registration and tackle negative perceptions of electoral fraud by introducing a requirement for people to register individually and provide personal information, which is then used to verify the entitlement of the person making the application to be registered. Only those persons who pass the verification checks will be added to the register.

Requirement to Share Data

Legislation that enables the matching of local authority data disclosed to EROs for maintaining the accuracy and completeness of electoral registers requires that data must be shared only in accordance with instructions (or an agreement between the ERO and the local authority whose data is to be used). The instructions or agreement will impose requirements for the processing of the information, including requirements as to its transfer, storage, destruction and security. They will also make provision for the consequences of a failure to comply with such requirements.

Data Management

Data may be shared between local authorities for the purposes of verification, entitlement to be included on the electoral register and electoral administration only. IER will provide an opportunity to support the completeness and accuracy of the register by tackling under-registration through local data matching. Local data matching will be carried out locally by EROs and their staff and data may be shared amongst two tier authorities to aid this activity; however, personal data will be shared

only for data matching purposes to determine if an elector has provided genuine information on their application and for ensuring the accuracy of the register.

The only exemptions and exceptions that will be lawful under IER are those that are permitted under existing legislation, for example disclosure of information for the purposes of law enforcement. It should be noted that paragraph 1A of schedule 2 to the Representation of the People Act 1983 ("Sharing and checking information etc") provides that provision made under the paragraph has effect despite any statutory or other restriction on the disclosure of information.

Public Impact

The information will be collected from every person who makes an application to register to vote in Great Britain. It will be compulsory to provide information to verify an application in order to register. However, the use of data matching to confirm existing electors on the register on the transition to IER will mean that a substantial majority of the electorate will be transferred to the individual register without having to re-register and provide their personal information.

Public Awareness

A public campaign run by the Electoral Commission will communicate the need to provide additional information when registering to vote through IER. From 10th June 2014 (in England and Wales) and 19th September 2014 (in Scotland) the application form for electoral registration will require additional information in order to allow verification of applications. As part of IER registration individuals will be provided with a fair processing notice explaining how their data will be used.

Individuals will have access to their own data through the standard procedures under the Data Protection Act. Those who do not wish to, or cannot, provide this information through one of the main channels, will be offered alternatives such as attending in person and providing alternative documentation.

Technologies - Electoral Management Systems

The Cabinet Office and the Government Digital Service have worked with electoral management suppliers to ensure security and privacy requirements for data transfer for IER are met. All data transfers via the Electoral Management Systems (EMS) are carried out on secure networks, the users of which are required to comply with the appropriate Code of Connection.

Technologies used for IER will not increase the potential for invasion of privacy. Information technologies will be used to compare personal identifiers supplied with the consent of the applicants against information held by the Department for Work and Pensions (DWP). The data safeguarding arrangements for verification and confirmation will be clearly articulated in a Data Sharing Instructions issued by the Lord President. Data safeguarding arrangements for the confirmation process are

clearly articulated in Data Sharing Instructions imposed by the Lord President in accordance with Regulation 4 of the 2013 Regulations, and all taking part will in any case be required to comply with the applicable provisions of the Data Protection Act throughout.

How Individual Electoral Registration will work in East Staffordshire Borough Council

Confirmation

On a date assigned by Cabinet Office the ERO will, as provided by the Electoral Registration and Administration Act 2013 (Transitional Provisions) Order 2013 (S.I. 2013/3907), as amended by the Electoral Registration and Administration Act 2013 (Transitional Provisions) (Amendment) Order 2014 (S.I. 2014/449), supply to Cabinet Office on behalf of the Lord President of the Council, via the IER DS an extract from their electoral register. This data will be transferred to DWP via the IER Digital Service for processing.

DWP will compare the extract of the electoral register and provide to the ERO, via the IER DS, a matching report for each of the entries. The Cabinet Office will publish an evaluation following the completion of confirmation.

Verification

The objective of verification is for EROs to assure themselves that an applicant for electoral registration is who they claim to be. In order to achieve this, the personal details provided by an applicant for registration will be matched against records held by DWP.

Verification will involve assessing certain personal data of electors or applicants who have applied for inclusion on the electoral register and comparing that with the personal data held by a Government department. EROs and their staff and central government officials involved in verification are accustomed to managing and processing personal data and are familiar with the legal and administrative requirements for doing so. The storage and handling of data will be closely controlled and data provided in relation to an individual for verification will comprise:

(a) Information which already appears on the electoral register if the individual concerned is on the register, i.e. electoral number, first name; last name; middle name; whether included in the edited register; current address; current postcode; current Unique Property Reference Number (information kept in the same database and which relates to the source, collection or recording of an item of data (e.g. the date on which an address was last updated) will also be provided); and

(b) Additional information provided with the consent of the individual concerned, i.e. National Insurance number, date of birth, previous address, previous Unique Property Reference Number, previous postcode and previous surname where relevant.

Data to be collected

The data that will be collected from each elector making an application under IER is:

- Full name (first name, middle name, family name, previous name used in last 12 months)
- Full residential address, including postcode
- Nationality
- Declaration of truth (a declaration that all information provided is true)
- Date of birth (new requirement)
- National Insurance number, where possible (new requirement)
- Any other residence, including an address where they are currently registered (new requirement)
- Any previous address in the last 12 months (new requirement)

In some cases additional information may be collected from applicants for registration. This information may include:

- Passport number (in cases where the ERO has exercised his or her power to request additional evidence where certain information is unavailable or where he or she considers it necessary)
- Service number (where the applicant is applying to be registered in pursuance of a service declaration)

Information of a personal nature will be collected on individual forms – including date of birth and National Insurance number.

Nationality information will also be collected (whilst this is not considered sensitive personal information, it can provide an indicator of ethnic origin and so will be treated with the same care).

Nationality and passport number may be collected in order to establish an individual's identity and determine eligibility to register to vote, but will not be used for matching or be included in the register.

For those who do not have a National Insurance number or who cannot be matched against DWP records, regulations provide alternative options to enable electoral registration. EROs will be able to use their existing power to use data already held by their local authority or county council in order to verify applicants. Regulations also provide a documentary exceptions process that allows applicants to provide identity documents, such as a passport or UK driving licence, in support of their

application. Applicants who cannot prove their identity by any other means may supply an attestation of their identity by a person of good standing in the community.

It is important to note that although additional information will be collected this will not form part of the electoral register. The information currently captured on the electoral register will remain the same. The regulations enabling the collection of this, and all data required for IER, provide clear guidelines about its retention and destruction.

Risk Overview

This process has involved both formal and informal engagements to determine the risks to personal data and controls and mitigation strategies to manage these risks.

National Insurance numbers and other personal details will be provided by individuals to assist in the verification of applications. The identity of "at risk" electors who may suffer physical harm if they are found (e.g. anonymous electors) will be protected at all times.

A person's ability or inability to present certain personal information for the purposes of verification is not a determining factor of their right to register, e.g. if a person does not have a National Insurance number, it will not prevent them from registering to vote, as alternative methods of verification will be available.

A significant amount of work has been conducted with various stakeholders on the security risk to personal information and appropriate mitigation strategies which have been, and will continue to be, incorporated into policy and business processes.

What security levels are involved?

IER will be classed as a security Level of OFFICIAL as it involves the collection of personal data. Further information on security levels can be found atwww.cesg.gov.uk.

Data transfers will comply with OFFICIAL security levels allowing data to be transferred securely between local authorities and public sector departments either via GCSx (or equivalent) or PSN. Public Services Network is a shared IT network that provides an assured network over which government can safely share services.

Stakeholders/participants

The following organisations are stakeholders or participants in the IER process and should be considered in the assessment of data protection risks for the policy underlying the transition to IER:

- Electoral Registration Officer/s
- East Staffordshire Borough Council
- Xpress Software Solutions Limited
- Direct Network Service Supplier (IT related)
- The Cabinet Office
- Electoral Commission
- Association of Electoral Administrators
- Society of Local Authority Chief Executives
- The Information Commissioner
- DWP, DSDNI and HMRC
- FCO Services
- The Electoral Commission
- Elected Council Members
- Residents in the electoral area

Compliance with privacy requirements and the data protection principles

EROs will be subject to the terms of Data Sharing Instructions issued by the Cabinet Office with the approval of DWP, HMRC and DSDNI. The agreement will set out the arrangements for the transfer and matching of the data, including requirements as to its transfer, storage, destruction and security. The agreement must be concluded in writing before the ERO may disclose the information. EROs must comply with the relevant legislation[1] and HM Government information security standards[2], and with the eight data protection principles, which provide that data must be:

Data must be...	Compliance
Fairly and lawfully processed	Processing will take place only with the consent of those concerned (although this consent is limited by the fact that they are required to provide these details in order to register to vote). The ERO will use the data solely for the purposes of electoral registration. Only EROs and support staff will have access to data received from public authorities. Other council staff will not have access to this data. EROs will check, and if necessary update, their data protection registration with the Information Commissioner's Office in order to ensure that the registration reflects the exchange of data with central government departments.

[1] In particular: Data Protection Act 1998; Representation of the People Act (England and Wales) Regulations 2001; Representation of the People Act (Scotland) Regulations 2001; Electoral Registration and Administration Act 2013; Freedom of Information Act 2000.

[2] CESG Information Assurance Standards, in particular IS5 (Secure Sanitisation) and IS6 (Protecting Personal Data and Managing Information Risk).

Data must be...	Compliance
Processed for specific and lawful purposes and not further processed in a way that is incompatible with the original purposes	The ERO will use the data solely for the purposes of individual electoral registration and only as allowed by legislation.
Adequate, relevant but not excessive	Only the information required for the purposes of IER will be used.
Accurate and up to date	The DWP data is a trusted Government data source. However, the ability of DWP to provide accurate information for matching is based on the feeds of information from its own sources being informed of changes of a customer's circumstance. There may also be a time lag between a change of circumstances being notified to a feeder system and it appearing in DWP data. As in all cases, eligibility to register is at the EROs discretion and they may use local data or other evidence to make a determination about an applicant's eligibility to be included on the electoral register.
Not kept for longer than is necessary	Regulations and the data sharing instructions require that EROs securely destroy **National Insurance numbers** received for the purposes of IER within 13 months from the date on which the application is determined. The data to be securely destroyed includes the destruction of electronic mails, paper copies and all electronic copies. Printed material will be shredded, or disposed of in a sealed confidential waste container.
Processed in accordance with the data subject's rights	Data will be confidentially processed. No data about anonymous electors will be sent to DWP. DWP, DSDNI and HMRC sensitive customer records will not be matched with the personal identifier data submitted by the ERO.
Kept secure	All activities involved in IER must comply with applicable legislation and HM Government policy, including the Data Protection Act 1998; HM Government Security Policy Framework; and Government Information Assurance Standards, and the data sharing agreement to be signed by the ERO, Cabinet Office, DWP, HMRC and DSDNI. Data will be transferred and stored securely. Only named individuals will be authorised to transfer data. Protection of information training will be provided to

Data must be...	Compliance
	all staff involved before they have access to data used for IER.
Not be transferred to countries outside the EEA unless exemption applies or adequate protection is ensured	The data will not be transferred to countries outside the United Kingdom.

Risk management

The Government takes the handling of personal data and prevention of identity fraud very seriously. The changes to electoral registration are intended to prevent fraud and maintain the integrity of the electoral system. Below is an overview of the data protection, data sharing risks and controls and mitigation strategies:

Risk Description	Controls/Mitigation
Data security breach – data mishandled by registration officer or other authorised users.	Data handling instructions and/or agreements set out the requirements for the handling, transmission, security and destruction of the data. All staff handling personal data will have received the appropriate training. Engagement has taken place with IT suppliers to ensure systems are appropriate to protect data.
Data is used for unauthorised purposes or shared inappropriately.	Data sharing instructions will be in place governing the use and handling of data. Will conform to data protection principle that data must be processed for specific and lawful purposes. There are strict rules around the disclosure of information provided in connection with applications for registration or that received as a result of data matching. Legislation provides for an offence of unlawful disclosure of data, punishable on conviction on indictment with up to two years' imprisonment on conviction. The additional information collected as part of the electoral registration application will not appear on the electoral register. The details currently captured in the electoral register will remain the same.
Data is accessed by unauthorised persons.	Engagement has taken place with suppliers to ensure that systems are appropriate to protect data. Local Authorities have undergone PSN compliance which sets standards about security of buildings and staff training on information handling.
Inappropriate retention of the data.	Data sharing instructions set out timescales for the retention and destruction of data and conform to the

Risk Description	Controls/Mitigation
	data protection principle that data must not be kept for longer than is necessary. EROs will be required to securely destroy National Insurance numbers no later than 13 months from the date on which the application is determined.
Data received results in identification of fraudulent activity.	EROs will already have procedures in place for dealing with instances of suspected electoral fraud; data-sharing merely provides an alternative way in which such instances may be identified and existing procedures will be followed.
Access to the data – data matching leads to the identity of an anonymously registered elector being disclosed.	EROs are to ensure that anonymous electors are omitted from the data sent for confirmation matching.
Storage of the data received – inadequate storage of the data could lead to loss.	Data sharing instructions set out requirements for the storage of data and conform to the data protection principle that data must be kept secure.

Security Breach Process

Upon receipt of information indicating that there has been a security incident immediately:

The person notified of/responsible for the incident must contact ERTP-incident@cabinet-office.gsi.gov.uk immediately. This mailbox is routed to the IAO, Deputy IAO, and Security Accreditor.

The incident, with minimal detail, will be stored on ePIMS by one of the three people named above in the folder marked 'Security Incidents' and the file-name must follow the following format [ddmmyyyy_v1, ... 2, ...3].

As per the Cabinet Office Incident Management Policy, the following information must be gathered:

- What format (electronic or hard copy – and if the former what IT system is involved) was the data held on;
- What data was involved and whether it included protected personal information;
- What quantity and detail of data was involved;
- The security classifications of the material involved;
- What impact the breach could potentially have on the affected areas of the department concerned;
- What impact the breach may have on the Cabinet Office;

- What impact the breach may have on the originator of the documents (be it electronic or hard copy), other departments and potentially also the Government.

If there is a potential data breach the individual notified must report the above information to the DSU (jerry.page@cabinet-office.gsi.gov.uk (DSO); and john.bolster@cabinet-office.gsi.gov.uk (Deputy DSO)) within 24 hours of the incident occurring.

Incident details to be circulated between the IAO, the Deputy IAO, and the Security Accreditor named at the top of this section.

If there is a potential data breach and/or if the incident has any cause/effect on a user of the digital service or a stakeholder/supplier in the chain, the incident must also be reported to the PSNA (PSNA.servicebridge@cabinet-office.gsi.gov.uk). Other factors to consider before notifying the PSNA include whether or not the incident requires the co-ordination of multiple service providers within the PSN, or if the incident has disputed ownership. This report must be filled out in the style of the PSN approved template.

If the potential data breach has an effect on any other stakeholders, then they and the SAWG (composed of DWP, HMRC, CO, PSNA, VJB, and ERO representatives) should be informed once the initial summary has been compiled.

The incident report will be updated as the incident investigation is carried out. This investigation is to be carried out by the person the incident is reported to as promptly as possible.

When the incident report has been written up in full a summary should be sent to the SIRO and the DSU.

The incident report will be circulated around SAWG members and then fed into the monthly meeting for discussion and relevant action.

Contact details

For further information regarding the IER in East Staffordshire Borough Council please contact:
Elections Team 01283 508376 elections@eaststaffsbc.gov.uk
Nicky Gilligan Principal Elections Officer 01283 508332
Julie Murfin Senior Elections Officer 01283 508311