INFORMATION SHARING PROTOCOL

SUMMARY SHEET

Title of Agreement	EPPING FOREST DATA FOR ELECTORAL PURPOSES

Organisation Name	Head Office Address	Phone	Email	Named Data Protection Officer	ICO Notification reference
Essex County Council	County Hall, Chelmsford, CM1 1QH, UK	033301 30690	DPO@essex.gov.uk	Paul Turner	Z6034810
Electoral Registration Officer for the District of Epping Forest	Electoral Services, EFDC, Civic Offices, High Street, Epping, CM16 4BZ	01992 564023	wmacleod@eppingforestdc.gov.uk	Nathalie Boateng	Z5033101

Version Control	
Date Agreement comes into force	10 June 2021
Date of Agreement review	1 July 2022
Agreement owner (Organisation)	Electoral Registration Officer for the District of Epping Forest
Agreement drawn up by (Author(s))	Wendy MacLeod
Status of document – DRAFT/FOR APPROVAL/APPROVED	Approved by EFDC
Version	V1/05/21

Wider Eastern Information Stakeholder Forum

This Information Sharing Protocol is designed to ensure that information is shared in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing.

This protocol will help you to identify the issues you need to consider when deciding whether to share personal data. It should give you confidence to share personal data when it is appropriate to do so, but should also give you a clearer idea of when it is not acceptable to share data.

Specific benefits include:

- transparency for individuals whose data you wish to share as protocols are published here;
- minimised risk of breaking the law and consequent enforcement action by the Information Commissioner's Office (ICO) or other regulators;
- greater public trust and a better relationship by ensuring that legally required safeguards are in place and complied with;
- better protection for individuals when their data is shared;
- increased data sharing when this is necessary and beneficial;
- reduced reputational risk caused by the inappropriate or insecure sharing of personal data;
- a better understanding of when, or whether, it is acceptable to share information without people's knowledge or consent or in the face of objection; and reduced risk of questions, complaints and disputes about the way you share personal data.

Please ensure all sections of the template are fully completed with sufficient detail to provide assurance that the sharing is conducted lawfully, securely and ethically.

Item	Name/Link /Reference	Responsible Authority
Privacy Impact Assessment (PIA/DPIA)		
Supporting Standard Operating Procedure		
Associated contract		
Associated Policy Documents		
Other associated supporting documentation		

Published Information Sharing Protocols can be viewed on the WEISF Portal.

Commented [PM1]: Is this to be completed by us or ECC? What's our responsibilities here?

1.	Purpose	REFERENCES
To enable Essex County Council to disclose to the Electoral Registration Officer for the District of Epping Forest information it holds in respect of registered users of Essex Libraries within the District of Epping Forest, Blue Badge Disabled Parking Scheme and those receiving Adult Social Care from Essex County Council in the District of Epping Forest. The information identified is to be disclosed for the sole purposes of electoral registration. The information provided would be processed for the following purposes: (a)to verify information relating to a person who is registered in the electoral register or who is named in an application for registration in, or alteration of, a register, (b)to ascertain the names and addresses of people who are not registered but who are entitled to be registered, or (c)to identify those people who are registered but who are not entitled to be registered. (d) general in pursuance of the duty of the electoral registration officer to maintain an accurate and up to date register of electors as required by section 9A of the Representation of the People Act 1983. Based on the outcome of the use of the supplied information and the assessment of it against (a)-(c) above, individuals may be contacted to invite them to register as an elector, to advise them that a review of their registration at a given address is being undertaken and/or to advise them that their registration is intended to be removed. The purpose of the local data matching is to match electors already on our register and addresses with local or national data sources so that where there is a “match” with a data source, that property is sent a simple letter confirming the details we hold. This letter only needs a response if the elector needs to make a change. The more properties we can send down this route the better for everyone concerned. If we can’t achieve a “match” once all avenues of data matching available have been used, we have to send a different letter which does require a response and which we have to chase up if no initial response is received. No onward disclosure of the information from Essex County Council will take place to Epping Forest District Council (although Epping Forest District Council is a data processor for the data within the strict parameters of that processor role). The data will be securely deleted 3 months after it has been provided as those identified tasks will have taken place in that timeframe. The provision of the data shall be twice yearly in June and January.	GDPR Go to article 5
2.	**Information to be shared**	

Agency Name	Data field/description
Essex County Council	• **Name**
	• **Address**
	• **Date of birth**
	• **Nationality**
	• **Email Address**
	• **Telephone numbers**

GDPR
Go to articles 6 - 9

3. Legal Basis

General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018.

GDPR
Go to articles 6-14

Personal Data (identifiable data)	**Special Categories of Data (Sensitive identifiable data)**	**Law Enforcement data (e.g. community safety partnerships)**
Article 6: ***[please click and select]***	**Article 9**: (if appropriate): ***[please click and select]***	**DPA Part 3** (if appropriate): *[please click and select]*
Public Task	Choose an item.	Choose an item.
Legal Obligation	Choose an item.	Choose an item.
Choose an item.	Choose an item.	Choose an item.

Other legislation or statute as follows
The Representation of the People (England and Wales) Regulations 2001 – Regulation 35
Electoral Registration and Administration Act 2013 – Schedule 2 – Paragraphs 1 and 2.
The Representation of the People (England and Wales) (Amendment) Regulations 2014 – Regulations 2 and 3

4. Responsibilities

GDPR

For the purposes of this Protocol the responsibilities are defined as follows: For help go to https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN Articles 24 – 29 where these roles are explained.	Tick box	Organisation Name(s)	Go to articles 13-14, 24 - 31
The Sole Data Controller for this sharing is:	☒	Essex County Council	
The Joint Data Controllers for this sharing are:	☐		
In the case of **Joint Data Controllers**, the designated single contact point for Individuals is:	☐		
Data Processors party to this protocol are (please list):	☒	Epping Forest District Council Civica Electoral Services	

This Protocol will be reviewed one year after it comes into operation to ensure that it remains fit for purpose. The review will be initiated by the Electoral Registration Officer for the District of Tendring

5. Subject Rights

Essex Partner Agencies' Information Sharing Agreements are made publicly available on the Wider Eastern Information Stakeholder Forum website to enable compliance with article 12 of the GDPR.

It is each Partner's responsibility to ensure that they can comply with all of the rights applicable to the sharing of the personal information. It is for the organisation initiating the ISP to identify which rights apply, and then each Partner to ensure they have the appropriate processes in place.

Subject Rights **Select the applicable rights for this sharing according to the legal basis you are relying on**	Processes are in place to enact this right - please check the box
GDPR Article 13&14 – **Right to be Informed** – Individuals must be informed about how their data is being used. This sharing must be reflected in your privacy notices to ensure transparency.	☒

GDPR
Go to articles 12 – 15

GDPR Article 15 – **Right of Access** – Individuals have the right to request access to the information about them held by each Partner	☒	GDPR Go to article 16 & 22
GDPR Article 16 – **Right to Rectification** – Individuals have the right to have factually inaccurate data corrected, and incomplete data completed.	☒	
GDPR Article 17 (1)(b)&(e) – **Right to be forgotten** – This right may apply where the sharing is based on Consent, Contract or Legitimate Interests, or where a Court Order has demanded that the information for an individual must no longer be processed. Should either circumstance occur, the receiving Partner must notify all Data Controllers party to this protocol, providing sufficient information for the individual to be identified, and explaining the basis for the application, to enable all Partners to take the appropriate action.	☐	
GDPR Article 18 – **Right to Restriction** – Individuals shall have the right to restrict the use of their data pending investigation into complaints.	☒	
GDPR Article 19 – **Notification** – Data Controllers must notify the data subjects and other recipients of the personal data under the terms of this protocol of any rectification or restrict, unless it involves disproportionate effort.	☒	
Article 21 – **The Right to Object** – Individuals have the right to object to any processing which relies on Consent, Legitimate Interests, or Public Task as its legal basis for processing. This right does not apply where processing is required by law (section 3). Individuals will always have a right to object to Direct Marketing, regardless of the legal basis for processing.	☒	
Article 22 – **Automated Decision Making including Profiling** – the Individual has the right to request that a human being makes a decision rather than a computer, unless it is required by law.	☐	
Freedom of Information (FOI) Act 2000 or **Environmental Information Regulations** (EIR) 2004 relates to data requested from a Public Authority by a member of the public. It is best practice to seek advice from the originating organisation prior to release. This allows the originating organisation to rely on any statutory exemption/exception and to identify any perceived harms. However, the decision to release data under the FOI Act or EIR is the responsibility of the agency that received the request.	☐	
6. Security of Information		
Security measures in place		GDPR articles 30 - 45
There are good quality access control systems in place	☒	
Paper information is stored securely	☒	
Paper and electronic information is securely destroyed with destruction log for electronic information	☒	

Laptops and removable media such as memory sticks are secured when not in use	☒
Technical security appropriate to the type of information being processed is applied	☒
Arrangements are in place to meet the requirements for confidentiality, integrity and availability	☒
Disaster recovery arrangements are in place	☒
Encryption of personal data is fully implemented	☒
Data minimisation has been considered	☒
Can pseudonymised or anonymised data be used to meet your processing needs?	☐
There are sufficient access controls for systems/networks in place	☒
Routine and regular penetration tests are carried out	☒
Article 40 Codes of Conduct are adhered to (where applicable)	☐
Appropriate security is applied to external routes into the organisation; for example, internet firewalls and remote access solutions	☒
Confirm entry in Records of Processing Activity	☒
Any risks associated with this data sharing have been assessed by your organisation and approval to proceed granted by your authorising signatories	☒
Additional measure 1 – please specify here – originating data destruction after only 3 months	☒
Additional measure 2 – please specify here -	☐

Personal information will be securely shared via **secure FTP site**

Partners receiving information will:

- Ensure that their employees are appropriately trained to understand their responsibilities to maintain confidentiality and privacy;
- Protect the physical security of the shared information;
- Restrict access to data to those that require it, and take reasonable steps to ensure the reliability of employees who have access to data, for instance, ensuring that all staff have appropriate background checks
- Maintain an up to date policy for handling personal data which is available to all staff
- Have a process in place to handle any security incidents involving personal data, including notifying relevant third parties of any incidents

- Ensure any 3rd party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

International Transfers (NOT APPLICABLE)

~~If any personal data is to be transferred outside of the EEA, please ensure you capture the relevant supporting adequacy decision for such a transfer here (articles 40-43).~~

~~Adequacy Decision in place https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en~~	~~Date of approval by EU Commission is:~~	~~[Provide hyperlink here]~~
~~ICO Approved standard contract clauses in place https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf~~	~~Date of approval by ICO is:~~	~~[Provide hyperlink here]~~
~~ICO Approved Binding Corporate Rules in place https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/~~	~~Date of approval by ICO is:~~	~~[Provide hyperlink here]~~
~~The Individuals have given explicit consent to the transfer and understand the risks associated with the transfer~~	~~Confirm this consent has been recorded appropriately~~	~~√ / ×~~
~~The receiving organisation in a 3rd country is bound by an approved Code of Conduct recognised by the EU~~	~~Date of approval by ICO is:~~	~~[Provide hyperlink here]~~

ICO guidance on International Transfers can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

7. Format and Frequency

- The format the information will be shared in is **CSV OR EXCEL SPREADSHEET**
- The frequency with which the information will be shared is **TWICE A YEAR UPON REQUEST FROM THE ELECTORAL REGISTRATION OFFICER IN JUNE AND JANUARY.**

If a shared system is being used by partners:

- What system is being shared? **NONE**
- Who is the owner of the system? **NOT APPLICABLE**

8.	Data Retention	
Information will be retained in accordance with each partners' published data retention policy available on their websites, and in any event no longer than is necessary.		GDPR Go to article 5

9.	Data Accuracy	
Please check this box to confirm that your organisation has processes in place to ensure that data is regularly checked for accuracy, and any anomalies are resolved ☒		GDPR Go to articles 5, 16 - 18

10.	Breach Notification	
Where a security breach linked to the sharing of data under this protocol is likely to adversely affect an Individual, all involved Partners must be informed within 48 hours of the breach being detected. The email addresses on page 1 should be used to contact the Partners. The decision to notify the ICO can only be made after consultation with any other affected Partner to this protocol, and notification to the ICO must be made within 72 hours of the breach being detected. Where agreement to notify cannot be reached within this timeframe, the final decision will rest with the Protocol owner as depicted on page 1 of this document. All involved Partners should consult on the need to inform the Individual, so that all risks are fully considered and agreement is reached as to when, how and by whom such contact should be made. Where agreement to notify cannot be reached, the final decision will rest with the Protocol owner as depicted on page 1 of this document. All Partners to this protocol must ensure that robust policy and procedures are in place to manage security incidents, including the need to consult Partners where the breach directly relates to information shared under this protocol.		GDPR Go to articles 33, 34, 77 - 84

11.	Complaints	

Partner agencies will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this protocol.		GDPR Go to articles 16 – 22 & 77
12.	**Commencement of Protocol**	
This Protocol shall commence upon date of the signing of a copy of the Protocol by the signatory partners. The relevant information can be shared between signatory partners from the date the Protocol commences.		
13.	**Withdrawal from the Protocol**	
Any partner may withdraw from this Protocol upon giving 4 weeks written notice to the WEISF administration team weisf@essex.gov.uk. The WEISF administration team will notify other Partners to the Protocol. The Partner must continue to comply with the terms of this Protocol in respect of any information that the partner has obtained through being a signatory. Information, which is no longer relevant, should be returned or destroyed in an appropriate secure manner.		
14.	**Agreement**	

This Protocol must be approved by the responsible person within the organisation (SIRO/Caldicott Guardian/Chief Information Officer).

Approver Name	Paula Maginnis
Organisation Name	Epping Forest District Council
Date of Agreement	10 June 2021

Please submit this Protocol to weisf@essex.gov.uk with list of approved signatories. The Protocol will then be published on weisf.essex.gov.uk.

Email approvals will only be accepted from an authorised signatory role from each organisation. Please see the list of authorised roles per organisation on WEISF.essex.gov.uk