



Valuation Office
Agency

Information Sharing Protocols

between

**Valuation Office Agency (an
Executive Agency of HMRC)**

and

Braintree District Council

Date: January 2017

Contents

i. Glossary

- 1. Introduction**
- 2. Parties**
- 3. Legal basis of provision and confidentiality**
- 4. Information use, handling, security and assurance**
- 5. Responsibilities under the Data Protection Act 1998 (DPA)**
- 6. Responsibilities under the Freedom of Information Act 2000 (FoIA)**
- 7. Intellectual property rights**
- 8. Issue management**
- 9. Security incidents or information breaches**
- 10. Termination**
- 11. Recovery costs**
- 12. Commencement and review of ISP**
- 13. Signatories**

Annex A. Version control

Annex B. Contacts

Annex C. Review history

i. Glossary

The Billing Authority or BA	Braintree District Council
CRCA 2005	The Commissioners for Revenue and Customs Act 2005
Data Controller	Has the meaning set out in section 1 of the Data Protection Act 1998.
Data Processor	Has the meaning set out in section 1 of the Data Protection Act 1998.
Data protection legislation	Means the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.
DPA	The Data Protection Act 1998
FoIA	Means the Freedom of Information Act 2000 and any subordinate legislation made under this Act together with any guidance and/or codes of practice issued by the Information Commissioner or Ministry of Justice in relation to such legislation.
Hardcopy	Computer output printed on a physical object, normally paper, or a record which can be read without the use of any device.
HMG	Her Majesty's Government
HMRC	Her Majesty's Revenue and Customs
LGFA 1988	The Local Government Finance Act 1988
ISA	The Information Sharing Agreement details the information being shared, the reason it is being shared and how it will be transferred.
ISP	The Information Sharing Protocol covers the overarching arrangements for all information shared.
Personal Data	Means information relating to a living individual who can be identified – (a) from the information, or (b) from the information and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. Personal data is categorised into: people personal data, property personal data or sensitive personal data, but is mainly either people personal data or property personal data.
Soft copy	An electronic or digital copy of some type of information, where the computer output can be displayed on a screen.
VOA	Valuation Office Agency

1. Introduction

- 1.1.** This Information Sharing Protocol (ISP) sets out the overarching arrangements for all information that is shared by the Valuation Office Agency (VOA) with the Billing Authority.
- 1.2.** This ISP will be supplemented by individual Information Sharing Agreements (ISAs) that detail the information being shared, the reason it is being shared and how it will be transferred.

2. Parties

2.1. The parties to this ISP are:

- The Valuation Office Agency (an Executive Agency of Her Majesty's Revenue and Customs), Wingate House, 93/107 Shaftesbury Avenue, London W1D 5BU.
- Braintree District Council, Causeway House, Braintree, Essex, CM7 9HB

3. Legal basis of provision and confidentiality

- 3.1.** The VOA will only share information when it is legally able to do so.
- 3.2.** The VOA is subject to the Commissioners for Revenue and Customs Act 2005 (CRCA) which covers the confidentiality of information held by the VOA, when it is lawful to disclose that information and legal sanctions for wrongful disclosure. The VOA is not permitted to disclose information except in certain limited circumstances, including, for the purposes of its functions, where there is a legislative gateway or with customer consent.
- 3.3.** Section 18(2)(a) CRCA 2005 allows sharing of information in support of a function as long as it is reasonable and proportionate to do so.
- 3.4.** The Billing Authority will treat all information supplied by the VOA as confidential even if this agreement is terminated.
- 3.5.** The terms of this ISP and any supplementary ISAs remain in force whilst the information is retained by the Billing Authority even if the agreements have been terminated.
- 3.6.** Both organisations are legally obliged to handle personal data according to the requirements of the Data Protection Act 1998 and the Human Rights Act 1998.

4. Information use, handling, security and assurance

- 4.1.** Information will be managed by the Billing Authority (BA) in accordance with HMG's Security Policy Framework and in accordance with the principles of the ISO27001 Information Security Management System standard. It is not a requirement of this ISP for the Billing Authority to have actual ISO27001 certification, but the BA's systems must meet the required standards.
- 4.2.** The Billing Authority shall ensure that they have the relevant security and technical measures in place so that the network over which VOA information is exchanged is secure.

4.3. The Billing Authority will not disclose to any outside organisation VOA information except with the explicit prior consent of the VOA.

4.4. The information must be transferred securely to the Billing Authority with the prior agreement and approval of the VOA Information Security Manager.

4.5. On receipt of information supplied by VOA, the Billing Authority will ensure that they:

- only use the information for the purpose that it was provided;
- store information received securely, and in accordance with central government standards and in accordance with the principles of ISO27001, for example, in secure premises and on secure IT systems;
- ensure that only people who have a genuine business need to see the information will have access to it (reviewing the access at frequent intervals), that these individuals have received appropriate training and that they have undergone the appropriate level of security clearance;
- follow Cabinet Office guidelines when dealing with the information according to the Government Security Classification (GSC) scheme as classified by the VOA;
- report any information losses, wrongful disclosures or breaches of security relating to the information supplied by the VOA to the designated contacts immediately (within two days of becoming aware). This includes advising and consulting with the VOA on the appropriate steps to take, e.g. notification of the Information Commissioner's Office; contact details are security@voa.gsi.gov.uk tel 03000 500681. The VOA reserves the right to suspend information transfers in the event of a security breach or wrongful disclosure until the breach or wrongful disclosure has been resolved to the satisfaction of the signatories of this ISP and any relevant ISAs. The VOA can advise on how to send any sensitive details of the incident on secure channels;
- only hold information while there is a business need to do so and destroy it in line with HMG Security Policy Framework and the principles of ISO27001. This must include the secure destruction/deletion of information in both hard and soft copy;
- regularly review any risks to the information and the effectiveness of measures taken to mitigate those risks.

4.6. On request, the Billing Authority will provide written assurance (for example, a certificate of assurance) that they have complied with these undertakings. The VOA reserves the right to audit the Billing Authority's compliance with the requirements of this ISP, subject to prior notification. Where audit checks are carried out, the VOA will require the cooperation of the Billing Authority to provide the necessary evidence or outputs to demonstrate compliance. Should the VOA become aware of any areas of non-compliance, the VOA will:

- a) discuss and agree the areas of non-compliance with the Billing Authority
- b) agree remedial action with the Billing Authority to address the non-compliance within an agreed reasonable timeframe
- c) review and reassess compliance once the agreed remedial actions have been completed.

5. Responsibilities under the Data Protection Act 1998 (DPA)

5.1. Information supplied under this ISP and ISAs may contain personal data. Under the Data Protection Act 1998, personal data is information which relates to a living person whose identity can be deduced from it by itself or in combination with other information held by

the Billing Authority.

- 5.2.** The Billing Authority must comply with the Data Protection Act 1998 when handling personal information.
- 5.3.** The Billing Authority must obtain prior approval from the VOA should information be transferred to a country or territory outside the UK (contact: VOA IT Security; see Annex B).
- 5.4.** For the purposes of the Data Protection Act 1998, the VOA is the Data Controller of the data it shares with a Billing Authority until such time as the data is accepted into the Billing Authority IT systems. From this point the Billing Authority becomes the Data Controller as defined under the Data Protection Act 1998.
- 5.5.** A breach of the Data Protection Act 1998 may result in a monetary fine of up to £500,000, prosecution or other measures imposed by the Information Commissioner's Office.

6. Responsibilities under the Freedom of Information Act 2000 (FoIA)

- 6.1.** Information held by the VOA for its functions that either directly identifies a person or enables their identity to be deduced from it, is exempt from disclosure under s44 of the FoIA as it is prohibited by s23 CRCA 2005. Additionally s63C LGFA 1988 makes information relating to a person disclosed under s63A or s63B LGFA 1988 exempt information by virtue of s44 of the FoIA. As a result, such information should be protected from such disclosure when in the Billing Authority's possession.
- 6.2.** Should the Billing Authority receive a request under the FoIA for any of the information provided, the Billing Authority must make the VOA aware where information relates to a living person or whose identity can be deduced from it.
- 6.3.** The VOA and the Billing Authority will cooperate with each other in order to ensure any requirements under the FoIA are met.
- 6.4.** Requests under the FoIA must be replied to within 20 working days.

7. Intellectual property rights

- 7.1.** This ISP precludes the use of the following:
 - departmental or public sector organisation logos except with the explicit consent of the VOA
 - the VOA's name in press reports or social media mentions except with the explicit consent of the VOA.
- 7.2.** Information supplied by the VOA may include information from Royal Mail Postcode Address Finder (PAF®).
- 7.3.** Royal Mail Group Limited is the owner of intellectual property rights in the database known as PAF®. Where elements of PAF are within the information supplied, the Billing Authority are not given any right to use PAF by virtue of this ISP.
- 7.4.** Information supplied by the VOA is in Crown ownership and protected by Crown Copyright and Crown Database rights.
- 7.5.** Information supplied by the VOA may include the National Address Gazetteer Unique Property Reference Number (UPRN) which is licensed to Her Majesty's Revenue and Customs (HMRC) and the Valuation Office Agency (VOA) by Ordnance Survey. It is

expected that the Billing Authority will hold their own end licence before using the information. The VOA will only supply the UPRN information with the prior approval obtained from GEOPLACE.

8. Issue management

- 8.1.** Any issues must be reported to the designated contacts (or successors to the role) listed in Annex B.
- 8.2.** If it is not possible to resolve an issue within 10 working days and/or the issue may potentially have a negative impact on either the VOA or the Billing Authority, it will be escalated to the respective senior management teams.
- 8.3.** The senior management teams will be briefed on the issue including what steps have been taken to resolve the issue and any remaining barriers. They will agree any further action which could include contingency arrangements and negotiating agreed solutions.

9. Security incidents or information breaches

- 9.1.** Any incident or breach involving VOA information (such as loss or wrongful disclosure) must be reported to the VOA's nominated security contact within two working days of becoming aware.
- 9.2.** The report must explain the incident in detail and the steps that are being taken to address the incident. The VOA can advise on how to send any sensitive details of the incident on secure channels.
- 9.3.** On receipt of any security incident report the VOA will consider whether the impact means further transfers of information will be halted.
- 9.4.** The VOA reserves the right to suspend information transfers in the event of a security incident, information breach, or wrongful disclosure until this has been resolved to the VOA's satisfaction.

10. Termination of agreements

- 10.1.** Either party may terminate this ISP or any ISAs by giving 30 days' notice.
- 10.2.** The VOA reserves the right to terminate this ISP or any ISAs with immediate effect in the event of a security incident or information breach. However, where appropriate, the Billing Authority/VOA will seek to resolve any issues associated with a breach or an incident and each party will attempt to negotiate a settlement in the spirit of joint resolution as described in Clause 8.
- 10.3.** If the Billing Authority no longer requires information provided by the VOA, they must inform the VOA so that transfers can be halted. The Billing Authority must securely destroy all information in both hard and soft copy, including removal from any datasets when there is no longer a business need to retain it.
- 10.4.** If changes to this ISP are needed, notification should be sent to the VOA contact listed in Annex B.

11. Recovery costs

- 11.1.** The VOA reserve the right to recover any costs associated with producing and transferring information, which will be detailed in each ISA.

11.2. Costs must be notified and agreed between the VOA and the Billing Authority in advance of any information being delivered.

12. Commencement and review of ISP

12.1. This ISP will come into force from the date it is fully signed by both the VOA and the Billing Authority.

12.2. This ISP will be reviewed by both parties on a three yearly basis from the date of the document shown on the first page.

12.3. Reviews of this ISP can be called at any time by representatives of either organisation as listed in Annex B.

12.4. Annexes A, B and C can be updated without the need to validate through signature.

13. Signatories

Signed on behalf of the Valuation Office Agency

Signature  Print Name Adrian Ball

Position Director, Information and Analysis

Date 13/01/2017

Signed on behalf of

Signature  Print Name Ian Hunt

Position Head of Governance

Date 2/2/17

Annex A - Version History

Version	Date	Summary of changes
1.0	June 2016	Creation
1.1	October 2016	VOA update
1.2	October 2016	VOA review
2.0	December 2016	Final - shared
2.1	January 2017	Final - published

Annex B - Contacts

Contact	Email address	Responsibility
VOA: Security	security.offshoring@voa.gsi.gov.uk	Approval for off-shoring information outside the UK
VOA: Security	security@voa.gsi.gov.uk	Security and security incidents
VOA: LARM Team	ratesretention@voa.gsi.gov.uk	Reporting and escalating issues
VOA: ILD Team	imd@voa.gsi.gov.uk	Review and amendments to ISAs
VOA: ILD Team	foi@voa.gsi.gov.uk	FoIA requests
The Billing Authority	nicri@braintree.gov.uk and ian.hunt@braintree.gov.uk	Review and amendments to ISAs and other matters.

Annex C - Review history

Version	Date	Summary of Changes
2.1	January 2017	FINAL VERSION
2.2	January 2018	First review planned