

## **INFORMATION SHARING PROTOCOL**

between

**THE HIGHLAND & WESTERN ISLES VALUATION JOINT BOARD**, constituted under the Valuation Joint Boards (Scotland) Order 1995 and having its principal offices at Moray House, 16-18 Bank Street, Inverness, IV1 1QY (hereinafter referred to as "HWIVJB")

and

**COMHAIRLE NAN EILEAN SIAR**, a Scottish local authority having its principal offices at Council Offices, Sandwick Road, Stornoway, Isle of Lewis HS1 2BW (hereinafter referred to as the "Council")

**collectively referred to as "the Parties."**

### **1. INTRODUCTION**

The HWIVJB undertakes the functions of Electoral Registration and Valuation for the local government area of the Council.

The Assessor is appointed in terms of Section 27 of the Local Government etc (Scotland) Act, 1994 to undertake the duties of Electoral Registration Officer in the Council area for the purposes of the Representation of the People Act 1983. In terms of Section 58 of the Local Government etc. (Scotland) Act 1994, the Council and the HWIVJB have agreed that all the activities and services which the Council would have carried out under Sections 8 to 13 (inclusive) and Sections 52 to 57 (inclusive) of the Representation of the People Act 1983 are carried out by the HWIVJB.

The Electoral Registration Officer in respect of the Council area is the Assessor appointed in terms of Section 27 of the 1994 Act for the Council area.

Under the Lands Valuation Acts, principally the Lands Valuation (Scotland) Act 1854 and the Valuation and Rating (Scotland Act) 1956, the Assessor is responsible for the valuation of all non-domestic properties and for the valuations required for the council tax legislation, namely the Local Government Finance Act 1992, for the Council area.

The Parties require to share information in order for these functions to be carried out.

It is a fundamental principle of this Information Sharing Protocol that the confidentiality of the information shared between the Parties is paramount. The Parties agree to use their best endeavours to safeguard the confidentiality of the Personal Data.

As noted above, HWIVJB is comprised of both the Assessor and the Electoral Registration Officer. The Assessor is responsible for the valuation of all commercial and domestic properties within the Council area. The Assessor is also the Electoral

Registration Officer for the Council area with responsibility for compilation and maintenance of the Electoral Register. Depending on the statutory responsibility being undertaken, the Data Controller could be (i) HWIVJB; (ii) the Assessor; or (iii) the Electoral Registration Officer. It should be clear who the Data Controller is dependent on the information being shared, but where there is any doubt, this will be clarified between the Parties as required.

It should also be noted that the Council will be acting on behalf of the Chief Executive in its role as Returning Officer or Counting Officer in relation to Electoral information and the Chief Executive will be the Data Controller in respect of that information.

The parties will share Personal Data to enable the statutory functions outlined above to be carried out. This will include, but is not limited to:

- The Electoral Register
- Valuation Roll
- Council Tax Valuation List
- Tenancy/Occupier Information
- Local Data Matching
- Education Lists (to attest applications for inclusion on to the Electoral Register for 14 - 18 year olds)
- Non-Domestic Property Information (including but not limited to floor areas of properties)
- Domestic Property Information (including but not limited to floor areas of properties)

Information will be shared by a secure email between known parties, secure file transfers (including data sharing portals) and zipped files.

## **2. DEFINITIONS**

In this Information Sharing Protocol, the following words have the meanings stated.

- 2.1 "Controller" "Personal Data" "Processor" and "Processing" have the meaning set out in Data Protection Laws.
- 2.2 "Data Protection Laws" shall mean the Data Protection Act 2018, UK General Data Protection Regulation, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications) and any legislation that, in respect of the United Kingdom, replaces, or enacts into domestic law, GDPR or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.
- 2.3 "ISP" means this Information Sharing Protocol.

### **3. PURPOSE**

3.1 This ISP is intended to:

- Enable information sharing for the functions undertaken by the HWIVJB in accordance with relevant legislation.
- Set out the principles which underpin the exchange of information between the Parties, particularly to ensure compliance with Data Protection Laws.
- Define the specific purposes for which the Parties have agreed to share information.
- Describe the roles and structures which will support the exchange of information between the Parties.
- Describe the arrangements which have been agreed for exchanging information.
- Describe the security procedures necessary to ensure that the confidentiality of information exchanged is maintained.
- Set out the responsibilities of the Parties.
- Provide staff with clear guidelines on the information sharing.

### **4. KEY LEGISLATION**

- 4.1 Data Protection Laws require that the Processing of Personal Data complies with the data protection principles. The Parties acknowledge that for the purposes of Data Protection Laws each Party is a Controller and determines how and why personal data are used for each stage of this information sharing project. The Parties further agree that they will ensure that their Processing of Personal Data shall be in accordance with Data Protection Laws. Information shared under this ISP will be processed only for the purposes for which it is supplied, as follows:
- 4.2 Personal Data will be kept confidential by the parties and must not be disclosed to any third party, except in accordance with clauses 4.3 and 4.4 or used for any secondary purposes whatsoever without the written consent of the other party.
- 4.3 Personal Data may be disclosed to, or a secondary use made of that data by the third party, where the Party disclosing is obliged to disclose as a result of a court order or of a statutory duty obliging such disclosure. The

disclosing Party shall notify the other Parties of any third party disclosure it is required to make in terms of this clause, who shall, as soon as reasonably practicable, confirm whether they wish to challenge the court order or statutory duty and provide the legal basis for doing so. For the avoidance of doubt, this clause does not apply to third party disclosures in terms of electoral legislation, whereby candidates, agents, parties are able to request copies of the electoral registers and absent voters lists from the Electoral Registration Officer. Nor does this clause apply to these parties obtaining copies of marked registers and marked postal voters list following an electoral event.

- 4.4 Should any Party receive a subject access request under Data Protection Laws, it must give careful consideration to those Laws. If in any doubt as to whether the Personal Data shared under this Agreement should be disclosed to the data subject, the other Parties should be consulted, as relevant.
- 4.5 It is the responsibility of each Party to ensure that relevant staff within each of their organisations are given appropriate training on the legislative requirements in relation to data protection.

## **5. ACCESS AND SECURITY PROCEDURES**

- 5.1 Formal policies and procedures must be in place addressing the physical security of buildings, security awareness, training of staff and security management of systems, both manual and electronic where identifiable information may be held.
- 5.2 Access to Personal Data shared under this ISP must be restricted by Parties to their staff on a need to know basis in connection with the purpose of this ISP. Each Party undertakes to ensure that their staff are aware of their obligations under Data Protection Laws and the limitations on use of Personal Data imposed by this ISP.
- 5.3 All staff that may receive or have access to Personal Data provided under this ISP must be background checked to confirm their identity, right of residence, qualifications, previous criminal convictions or any outstanding criminal prosecutions/investigations which would indicate that they should not be permitted access to information relating to this Agreement. Any documentation provided in support of the above should be original with no photocopies permitted.
- 5.4 Each Party undertakes to comply with Data Protection Laws, and in particular, warrants that appropriate technical and organisational measures shall be taken against unlawful or unauthorised Processing of Personal

Data shared under this ISP and against accidental loss or destruction of, or damage to, this Personal Data.

- 5.5 No term of this ISP, whether express or implied, shall preclude either Party from disclosing, if required, or considered necessary under the Freedom of Information (Scotland) Act 2002 ("the 2002 Act"), details of all matters relating to this ISP. The Recipient Party's interpretation of the 2002 Act and any exemptions therein will be final and conclusive. The Parties will facilitate one another's compliance with its obligations under the 2002 Act and comply with any request from the other Party for that purpose.
- 5.6 In exercising their obligations under the 2002 Act and any subordinate legislation or codes made under the 2002 Act, both Parties shall have due regard to the commercial interests of the other Party, but without prejudice to its duty to discharge its obligations in terms of the 2002 Act.

## **6. MANAGING THE INFORMATION**

- 6.1 Electronic transfer of personal information will only be permitted on a system to system basis across secure networks
- 6.2 Updates will be provided by either party to the other party when information or circumstances change. The Parties recognise the importance of good records management, in ensuring that information is regularly validated and refreshed. Inaccurate and out of date data is clearly detrimental to effective information sharing.
- 6.3 Fax, general post and unencrypted transfers should only be used where considered necessary and reasonable in the circumstances.
- 6.4 Removable and more mobile media such as CD roms, memory sticks or lap tops are generally prohibited. However, if an exceptional requirement arises, then the same encryption rules apply and delivery method must be by traceable secure courier service or hand delivery.
- 6.5 All information systems containing identifiable information must be effectively password protected. Users must not divulge their passwords, nor leave systems active while absent.
- 6.6 It is recognised that in urgent cases, information may have to be requested or provided via the telephone. Face-to-face transfers are also covered by this ISP. The Parties should ensure that their internal procedures reflect the provisions of this ISP.
- 6.7 Written communications containing personal information should be transferred in a sealed envelope and addressed by name to the designated person within each Party organisation. They should be marked "Personal

Private and Confidential – to be opened by the recipient only" and placed inside an addressed sealed envelope which does not carry any confidentiality markings. The designated person should be alerted to the despatch of such information and should make arrangements with their own organisation to ensure both that the envelope is delivered to them unopened and that it is received within the expected time scale. Where a Party has a policy that all mail is to be opened at a central point, prior to delivery to the named recipient, then this policy must be made clear to the other Party so that an alternative means of transfer can be adopted where it is essential that the information is restricted to those who have a need to know.

## **7. DISCLOSURE, RETENTION, ARCHIVING AND DISPOSAL**

- 7.1 Processing of any information provided under this ISP, other than for the purposes outlined within this ISP is not permitted. The recipient Parties will not otherwise exploit or disclose this data.
- 7.2 Information provided under this ISP will be retained for a period of no less than one year following termination of this ISP.
- 7.3 Archived areas must have, at the very minimum, access controls to secure the area and provide unauthorised entry be protected against water damage.
- 7.4 System audit logs must be retained for a minimum of twelve months.
- 7.5 Any disposal of data in accordance with clause 7.2 above must be securely destroyed in accordance with HMG Information Assurance Standards and confirmation should be provided to HWIVJB that the Data have been deleted.

## **8 INCIDENT MANAGEMENT**

Any risk to or compromise of HWIVJB information must be notified to HWIVJB within 24 hours. Any actual or apparent breach of Data Protection Laws by any employee of any Party involving data under this ISP will be investigated by that Party as a matter of priority. HWIVJB would be informed of the situation as soon as possible and will be kept up to date with the situation.

Any Party involved in such an information security incident must:

- Nominate a named senior manager to manage the incident and liaise with HWIVJB during any report of an investigation into a loss, compromise or damage to HWIVJB Information and
- facilitate any HWIVJB investigation into this matter.

## 9. ROLES AND RESPONSIBILITIES UNDER ISP

- 9.1 Each Party must provide a single point of contact (SPOC) who will work together to implement this ISP. The sharing of information will only take place where it is valid and legally justified having regard to the purpose and principles underpinning this ISP.
- 9.2 No later than 12 months from the date of signing of this ISP, the SPOCs will review the data held to ensure the data comply with the data protection principles, in particular, that the data are:
- adequate, relevant and not excessive in relation to the purpose for which the data are processed
  - accurate and, where necessary, up to date
  - not kept longer than necessary
- Data which do not comply with the above principles will where appropriate, be corrected or destroyed.
- 9.3 Information discovered to be inaccurate or inadequate for the specified purpose will be brought to the attention of the originator of the information. The originator will be responsible for correcting it and notifying the recipients of the corrections.
- 9.4 Each Party is responsible for maintaining records of the data sharing.
- 9.5 The Party sharing information will maintain a record of the information shared, including the date of disclosure and who authorised it.
- 9.6 The Party receiving information will maintain a record of the information received, including the date of receipt.

The SPOC for HWIVJB is:

██████████ Depute Electoral Registration Officer / Business Manager  
██████████

The SPOC for the Council is:

██████████, Governance and Elections Manager ██████████

## **11. REVIEW OF THE ISP**

The ISP will be reviewed twelve months after the implementation date and annually thereafter, but any party can request a review at any time, providing reasonable cause can be shown.

The review will be carried out by the SPOCs

The reviewers will consider whether the:

- ISP is achieving its purpose
- information sharing is operating smoothly
- contact details require updating

Any changes identified during the review must be agreed by all Parties to this ISP.

Any Party may request a copy of the Information Security Policy.

## **12. DURATION AND TERMINATION**

12.1 This ISP shall come into force immediately on being executed by both Parties.

12.2 This ISP shall last until terminated or superseded in terms hereof.

12.3 Notwithstanding the termination of this ISP, any duties of confidentiality imposed on the Parties or in respect of staff or agents hereunder shall subsist indefinitely.

12.4 Either Party may terminate this ISP on giving six months' written notice to the others of their intention to do so.

12.5 This ISP may be varied by the written agreement of the Parties.

12.6 Any Party may terminate this ISP by notice in writing immediately if:

- (i) another Party is in breach of any of the terms of this ISP which, in the case of a breach capable of remedy, shall not have been remedied by that other Party within 21 days of receipt of a written notice specifying the breach and requiring its remedy; or
- (ii) another Party is incompetent, guilty of gross misconduct and/or any other serious or persistent negligence in the carrying out of its duties hereunder.

12.7 The obligations on each Party under this ISP shall be continuing and, in particular, shall survive termination of the ISP.



12.8 Except expressly provided in this Agreement, no variation of this Agreement shall be effective unless it is agreed in writing and signed by both Parties.

**13. INDEMNITY**

Each Party shall indemnify and keep the other indemnified from and against all claims, damages, demands, expenses, losses and liabilities which may be incurred directly or indirectly in connection with a breach of this ISP, including any monetary penalty imposed by the Information Commissioner's Office but only to the extent that any such claim, etc is incurred as a result of the fault of the indemnifying party.

**14. DISPUTES**

The Parties agree to act in good faith at all times and attempt to resolve any disputes arising as a result of their respective rights and duties hereunder on an amicable basis.

**15. ASSIGNATION AND SUB CONTRACTING**

The Parties shall not assign or otherwise transfer by any means whatsoever, its rights and obligations under this ISP.

**16. NO WAIVER**

Failure to exercise, or any delay in exercising, any right or remedy provided under this ISP, or by law, shall not constitute a waiver of that, or any other right or remedy, nor shall it preclude or restrict any further exercise of that or any other right or remedy

**17. GOVERNING LAW**

This ISP shall be governed by Scots law and the Parties hereto submit to the exclusive jurisdiction of the Scottish Courts.

**We, the undersigned, agree to adopt and adhere to this Information Sharing Protocol:**

Authorised to sign for and on behalf of the  
**HWIVJB:**

Signature:



Name: 

Designation: Assessor & Electoral Registration Officer

Place of Signing: Inverness

Date: 13 September 2023

Witnessed by:

Signature:



Name: 

Designation: Admin Assistant/Secretary

Date 13 September 2023

Authorised to sign for and on behalf of  
**COMHAIRLE NAN EILEAN SIAR:**

Signature:



Name: 

Designation: Head of Law and Governance

Place of Signing: Stornoway

Date: 12 September 2023

Witnessed by:

Signature:



Name: 

Designation Executive Office Assistant

Date 12 September 2023