OPENNESS & CONFIDENTIALITY POLICY

APPROVED BY HHP BOARD:
August 2026
EFFECTIVE DATE:
August 2026

CONTENTS

INTRODUCTION

1.1 We aim to conduct our business in an open and accountable manner whilst, at the same time, ensuring that personal and commercial confidentiality is maintained where appropriate.

1.2 We believe that our members and any other interested parties should have access to information on how we conduct our business. As a general principle, information about HHP and our work should be widely and freely available. Requested information will be made available unless it is considered commercially sensitive, personally confidential or where disclosure is restricted by legislation.

1.3 Our staff and Board Members will:

a) treat all personal and sensitive organisational information as confidential to the Partnership;
b) comply with the law regarding the protection and disclosure of information including personal data;
c) process and disclose personal data only where there is an appropriate lawful basis under data protection legislation, and where required meet the additional conditions for special category or criminal offence data; and
d) not gain or attempt to gain access to information they are not authorised to have.

DATA PROTECTION

2.1 We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and related information rights legislation. These laws set out how personal data must be collected, used, stored, shared, retained and protected, and the rights of individuals in relation to their personal data.

2.2 All personal information relating to tenants, applicants, staff and Board Members that is not a matter of public record will be held in accordance with UK GDPR principles.

Lawfulness, Fairness & Transparency

2.3 Principle A of the UK GDPR states that personal data must be:

"processed lawfully, fairly and in a transparent manner in relation to individuals"

2.3.1 Under the UK GDPR we are required to identify valid grounds (known as a 'Lawful Basis') for collecting and using personal data.

2.3.2 Our Information Asset Register (IAR) outlines the various types of personal data of individuals that we process and shows the lawful basis for each information type. The IAR also identifies conditions for processing special category or criminal offence data. The IAR is reviewed regularly to ensure it remains accurate and up to date.

2.3.3 We will only process personal data in ways that individuals would reasonably expect, or where we have clearly explained the processing and have an appropriate lawful basis. Before introducing any new processing that is likely to result in a high risk to individuals' rights and freedoms, we will carry out a Data Protection Impact Assessment (DPIA) and implement any necessary safeguards.

2.3.4 The ***Transparency*** requirement is closely linked to the Right to be Informed which gives individuals extended rights in respect of being informed about the collection and use of their personal data.

2.3.5 Our privacy information, including our Privacy Policy and relevant privacy notices, will be made available to individuals at the appropriate point in our relationship with them, or as soon as reasonably practicable where personal data is obtained from another source.

2.3.6 We will provide privacy information and relevant policy documents in accessible formats on request, and through appropriate channels for individuals who do not use digital services. We will take reasonable steps, and where required make reasonable adjustments, so that information is accessible and understandable.

2.3.7 Individuals are entitled to request access to their personal data through a Subject Access Request (SAR). We will respond without undue delay and in any event within one month of receipt, subject to any lawful extension permitted by data protection legislation.

2.3.8 We may need to verify an individual's identity prior to disclosure, and exemptions may apply where permitted by law.

2.3.9 We will be clear, open and honest with individuals from the start about how we use their personal data.

Purpose Limitation

2.4 Principle B of the UK GDPR states that personal data must be:

"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes"

2.4.1 We have recorded our purposes for processing personal data in our Fair Processing Notices.

2.4.2 Personal data must not be used for a new purpose unless that purpose is compatible with the original purpose, the individual has been appropriately informed and, where required, a new lawful basis or additional condition has been identified.

2.4.3 Staff should familiarise themselves with our FPN and SFPN, and if any processing activity that is not documented in the Notices becomes a necessity, the DPO should be informed in good time to allow for updating the Notices and making them available to affected individuals.

2.4.4 Unauthorised or unidentified processing activities must be reported immediately in line with our data breach and incident procedures. We will assess each incident promptly and, where required by law, notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of a reportable personal data breach. Where required, we will also notify affected individuals without undue delay.

Data Minimisation

2.5 Principle C of the UK GDPR states that personal data must be:

"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"

2.5.1 We can only retain information that is sufficient to properly fulfil our stated purpose, has a rational link to that purpose, and we do not hold more than we need for that purpose. We also need to be able to demonstrate that we have appropriate data minimisation practices in place.

2.5.2 We cannot collect personal data on the off-chance it might be useful in the future. However, we may be able to hold information for a foreseeable event that may never occur if we can justify it. For example, it is reasonable for us to retain relevant information on individuals who are no longer tenants if they have left and have an outstanding arrear, in order that we might pursue that debt if they become tenants at a later date. If we are unable to pursue that debt, i.e. in a bankruptcy case, we would not be able to retain the information.

2.5.3 For special category data and criminal offence data, additional care must be taken to ensure that only the minimum amount of information necessary is collected, used and retained, and that appropriate safeguards are in place.

Accuracy

2.6 Principle D of the UK GDPR states that personal data must be:

"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"

2.6.1 We need to ensure that the personal information we process is not incorrect or misleading, and we need to keep it as accurate and up-to-date as possible.

2.6.2 If we discover that any personal data is incorrect or misleading, we will take reasonable steps to rectify or erase it without undue delay, having regard to the purpose for which it is processed.

2.6.3 We will consider and respond appropriately to requests to rectify inaccurate personal data, and where necessary we will restrict processing while accuracy is being assessed.

2.6.4 Staff and Board Members' personal details are checked annually when they complete Disclosure of Interest Forms and we request an annual update in respect of personal information from our Membership prior to the AGM.

Storage Limitation

2.7 Principle E of the UK GDPR states that personal data must be:

"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes

or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals"

2.7.1 We cannot keep personal data for longer than we need it. Our Data Retention Schedule outlines how long we should retain personal data.

2.7.2 In addition, our *Maintenance of House Files* procedure gives guidance on the personal data of tenants that we should retain.

Integrity & Confidentiality

2.8 Principle F of the UK GDPR states that personal data must be:

"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

2.8.1 In accordance with this principle, we must ensure that we have appropriate security measures in place to protect the personal data we hold.

2.8.2 Our Privacy Policy outlines our approach to storage of personal data in paper and electronic formats:

Paper Storage

If personal data is stored on paper, it must be kept securely so that unauthorised persons cannot access it. When it is no longer required and retention requirements have been met, it must be destroyed securely. If personal data requires to be retained on a physical file, that file must be stored in accordance with our records management and storage procedures.

Electronic Storage

Personal data stored electronically must be protected against unauthorised access, loss, destruction or damage. Where personal data is sent externally, approved secure transfer methods must be used. Personal data stored on laptops, tablets, removable media or other portable devices must be subject to appropriate technical and organisational safeguards.

2.8.3 In accordance with the above, and with our Information Communication Technology (ICT) Security Policy, access to personal information is controlled to ensure that it is only granted to users based on role, operational requirements, and the duration for which access is required. Any personal information which is in hard copy is stored in locked cabinets with restricted access. Any personal information which is held in electronic format is protected and appropriate security measures installed to only allow permitted usage. These measures include the use of multi-factor authentication, passwords, firewalls, secure networks and encryption.

2.8.4 Controlled, confidential or special category personal data must not be sent externally unless appropriate security measures are in place, such as encryption or another approved secure transfer method, in accordance with our ICT Security Policy and data sharing procedures. Failure to comply with this requirement may result in disciplinary action and, where relevant, incident reporting under data protection law.

FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

3.1 Since 11 November 2019, Registered Social Landlords (RSLs) are classed as public bodies for the purposes of the Freedom of Information (Scotland) Act 2002 (FOISA).

3.2 Tenants and other individuals can request information from RSLs that may not previously have been available to the public at large.

3.3 The Data Protection Officer is responsible for responding to FOI requests.

3.4 A FOI request must be responded to within 20 working days.

3.5 A Guide to Information, which is an index of the information we publish and how to access it, is available on our website at the following link:

Hebridean Housing Partnership - Guide to Information

3.6 If a requester is dissatisfied with our response to a FOISA request, they may request a review. Reviews will be responded to within 20 working days. If they remain dissatisfied following review, they may appeal to the Scottish Information Commissioner in accordance with FOISA.

3.7 Requests made under the Environmental Information (Scotland) Regulations 2004 (EIRs) will be handled in accordance with those Regulations, including applicable timescales, exceptions and review rights.

GENERAL PRINCIPLES AND PRACTICE

Communication of Information

4.1 Information will be available through a range of channels considered appropriate to the information in question. This will include our website (www.hebrideanhousing.co.uk), social media, Tenants Handbooks, regular newsletters and in document form on request from our Head Office, and where practicable, Area Offices.

4.2 We will also provide an opportunity prior to our AGM for tenants to ask questions about performance, service standards and other general matters.

4.3 We will ensure that, wherever possible and practicable, information available to the public will be written in Plain English. Every effort will be made to avoid unexplained acronyms, jargon and technical language where Plain English alternatives exist.

4.4 In order to overcome barriers caused by disability, sensory impairment, language difficulties, literacy issues and other communication needs, we will, where reasonably practicable, make information available on request in a range of accessible formats and languages. This includes taking reasonable steps and, where required, making reasonable adjustments to ensure that individuals are not disadvantaged in accessing information or services.

PUBLICATION OF INFORMATION

5.1 The following paragraphs outline the information that will be made available on our website and the steps we will take to ensure compliance with this policy. This list is not considered to be exhaustive.

Annual Report and Accounts

5.1.1 The Annual Report will contain standard information required by law and will also report Performance against Operational targets. Monthly performance information will be available on request. The degree that tenants feel they are kept appropriately informed will be explored in Tenant Satisfaction Surveys, and the Partnership will increase the amount of information being circulated if any of the surveys suggest this.

How to become a Board Member or influence decisions in other ways

5.1.2 A leaflet is available to explain the process of becoming a Board Member.

5.1.3 It is recognised that on occasion tenants may wish to influence certain decisions, or have their voice heard, without necessarily joining the Board. Tenant Board Panel meetings can facilitate this.

5.1.4 Furthermore, where tenant and stakeholder views are being sought, consultation documents will be posted on our website.

Policies & Procedures

5.1.5 We will make available all key policies on our website and at our offices' reception. Availability of this information will be publicised from time to time in our relevant publications.

Results of External Audit

5.1.6 The external auditor will present the audited accounts at the AGM and respond to any questions submitted prior to the AGM.

Registers

5.1.7 We maintain a number of Registers which are available for inspection at the following locations:

Available at our Head Office	**Available on our website and at our Head Office**
Register of Board Members	Board Members Disclosure of Interest Register
Entitlements, Payment & Benefits Register	FOISA Register
Staff Disclosure of Interest Register	
Membership Register	

Board Agendas & Minutes

5.1.8 Non-confidential Board Agendas will be made available on the Partnership's website at least 3 days prior to Board meetings.

5.1.9 Non-confidential Board meeting minutes will be made available on the Partnership's website once they have been signed off by the Chair of the meeting. This will generally be after the next scheduled Board meeting.

Complaints

5.1.10 Information about complaints and complaint outcomes may be made available in anonymised or statistical form, where appropriate. Personal information relating to tenants, staff or other individuals will not be published or displayed.

ACCESS TO MEETINGS

Annual General Meeting

6.1 In accordance with our constitution, we will hold an Annual General Meeting (AGM) to which all members of the Partnership will be invited. Our AGMs are also open to members of the public.

Ordinary Meeting

6.2 Our Rules and Standing Orders state that all agenda items at Board meetings shall be considered as non-confidential unless otherwise agreed.

6.3 Minutes, with any confidential items omitted, may be viewed on our website and at our offices by the general public. Printed copies of the minutes can be made available on request for individuals without access to the internet. Where such a request is made, we will provide the document(s) within 7 working days.

CONFIDENTIALITY

7.1 Our staff will generally have access to all information they require to carry out their work and are under a duty to respect the confidentiality of all personal information held by us.

7.2 Staff must explain, where appropriate, the purpose for processing an individual's personal data and, where relevant, any categories of recipients outside the Partnership who may receive it. Personal data must only be processed or shared where there is an appropriate lawful basis and, where applicable, additional conditions for special category or criminal offence data. Where the circumstances require it, consent must be obtained in a valid manner and recorded.

7.3 The following items are considered confidential and should, at no time, be divulged inappropriately – this is not an exhaustive list:

a) The personal data of tenants and other members of the public will be treated as confidential and will only be shared where there is a legitimate need, an appropriate lawful basis, and appropriate safeguards. Personal identifiers and unnecessary personal detail should not be included in Board reports or minutes unless there is a clear and lawful reason to do so;

b) Access to personal data records, whether paper or electronic, will be restricted to those who require access for a legitimate business, governance or legal purpose and who are authorised to do so. Any such access must be proportionate, properly controlled and recorded where appropriate; and

c) Items adjudged, on an ad hoc basis, to be confidential.

7.4 Exceptions to the items listed in paragraph 7.3 are:

a) where a tenant or other member of the public complains or appeals to us about an issue and a personal representation is being made to the Board as the final stage in the procedure. In these circumstances, it is impossible to withhold information on the person's identity.

b) where we have a legal obligation to provide information to a third party, in respect of, for example, the prevention of fraud.

Regulation

7.5 We may share personal data with third parties where this is necessary to deliver services, meet legal or regulatory requirements, or support performance monitoring and improvement. In such cases, we will ensure that information is shared lawfully, proportionately and securely, with appropriate contractual, data sharing and accountability arrangements in place. Where we act as data controller, we will remain responsible for ensuring compliance with data protection law.

Data Security

7.6 The following technical and organisational measures must be followed to protect personal data security:

a) All computer held personal data should be protected by biometric and multi factor authentication where available (when not available passwords, in line with our corporate password criteria, are required) and accessible only to staff with a legitimate need to access or process the data;

b) Computer systems should be secure and sufficiently protected against unauthorised access, and personal data should be encrypted or otherwise protected where appropriate;
c) Sufficient safeguards must be in place to protect computer-held personal data from loss, destruction, damage or unauthorised access. Special category data and other high-risk personal data must only be stored on laptops, tablets, removable media or other portable devices where this is necessary and approved safeguards are in place;
d) All back up information should be held securely, and protected against unauthorised access;
e) All personal data must be erased from PC's or other hardware and measures taken to protect it from subsequent retrieval by unauthorised persons on the disposal of such hardware;
f) Manual files containing personal data should be kept in secure filing cabinets when not in use – this includes returning files to locked cabinets overnight;
g) Care should be taken to ensure that manual files containing personal data are protected from loss or damage when removed from the office. Removing files from the office is discouraged and should only be done in exceptional circumstances. Under no circumstances should personal files be left unattended in vehicles;
h) Staff members printing tenants' personal data must print using the 'User Authentication' facility on the network and not leave the printer unattended while printing these documents;
i) All correspondence of a personal nature must have "Private and Confidential" clearly marked on the envelope;
j) Regular audits should be in place to test that technical and organisational security measures are being adhered to;
k) Staff working at home must work in a private environment ensuring conversations cannot be overheard.
l) Board Members attending meetings on MS Teams should be in private environment ensuring conversations cannot be overheard

Disposal of Personal Data

7.7 With regard to document retention schedules, when no longer required, all personal information, including computer printouts of rent accounts and arrears, must be securely shredded or otherwise securely destroyed in line with the Data Retention Schedule.

7.8 Data held on computers/electronic filing systems should be treated in the same manner as paper print-outs in respect of retention, and deleted accordingly.

7.9 The destruction of original records and documents, in both electronic and paper formats, should be authorised by managers and a file note must document this authorisation. The method of disposal should be appropriate to the confidentiality or sensitivity of the record.

7.10 Personal files should be checked regularly, and information only retained if still relevant to the purposes for which it was intended to be kept. This should be done as a matter of routine whenever files are in use.

BREACH OF POLICY

8.1 A breach of confidentiality, whether deliberate or inadvertent, will be considered a serious matter. All breaches will be dealt with via the Staff Disciplinary and Grievance procedures and the Board Code of Governance, taking all circumstances into account, and may result in:

a) the staff member(s) being issued with a warning or dismissed; or

b) the Board Member(s) being requested to leave the Board.

COMPLAINTS & APPEALS

9.1 Complaints regarding the policy will be dealt with under our Comments, Compliments & Complaints Policy, a copy of which is available at our offices and on our website.

9.2 Requests for review or appeals relating to Freedom of Information requests will be handled in accordance with FOISA. Requesters will be informed of their right to seek a review and, where applicable, to appeal to the Scottish Information Commissioner.

LEGAL AND REGULATORY FRAMEWORK

Legislation

10.1 In formulating, implementing and reviewing this policy, we will have regard to relevant statutory, regulatory and good practice requirements relating to information rights, openness, confidentiality, accessibility, equality and human rights.

10.2 The legislation particularly relevant to this Policy includes:

a) the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025: provide rights to individuals in relation to personal data held about them and regulate the collection, use, sharing, retention and security of personal data.

b) Freedom of Information (Scotland) Act 2002: entitles members of the public to request recorded information from a Scottish public authority, subject to certain exemptions. FOISA was extended to registered social landlords from 11 November 2019.

c) The Scottish Information Commissioner oversees FOISA and EIR matters, and complaints may be escalated to them where appropriate

d) Housing (Scotland) Act 2001, 2006, 2010 & 2014: provide a statutory right to all tenants with Scottish Secure Tenancies to receive information about their landlord's policies and procedures, in addition to obliging landlords to consult and provide tenants with information in developing their Tenant Participation Strategy. The 2010 Act introduced the Scottish Social Housing Charter which obliges landlords to consult with tenants in respect of desired standards and outcomes.

e) Scottish Public Services Ombudsman Act 2002: describes the statutory arrangements for conducting independent investigations of complaints relating to maladministration by a wide range of listed authorities, including Registered Social Landlords.

f) Human Rights Act 1998: gives individuals a right to respect for their privacy.

g) Environmental Information (Scotland) Regulations 2004: provide rights of access to environmental information held by Scottish public authorities, subject to specific exceptions.

h) Equality Act 2010: requires us to eliminate unlawful discrimination, advance equality of opportunity and foster good relations in the delivery of our services and functions, including by anticipating barriers, considering accessibility and making reasonable adjustments where required.

i) The Scottish Social Housing Charter and the Scottish Housing Regulator's regulatory framework: support openness, accountability, tenant communication, consultation and the provision of accessible information to tenants and other service users.

10.3 We will consider equality impacts when implementing and reviewing this policy, including the needs of people who may experience barriers because of disability, language, literacy, digital exclusion, sensory impairment or other protected characteristics. Where appropriate, we will use equality impact assessment processes to identify and address any adverse impacts.

TRAINING

11.1 The employee induction programme includes an overview of this policy, including responsibilities for the promotion and delivery of openness and confidentiality as relevant to their job descriptions.

11.2 Board Members and staff will receive updates on these issues and specific training on any specialised areas as required. Training needs are identified on an ongoing basis by various means including regular staff supervision sessions.

LINKS WITH OTHER POLICIES

12.1 The Openness & Confidentiality Policy is supported by related policies and procedures and should be read in conjunction with, but not limited to, the following:

- Code of Conduct for Staff;
- Code of Governance for Board Members;
- Communication Policy;
- Comments, Compliments & Complaints Policy
- Disclosure of Interest Policy;
- ICT Security Policy;
- Membership Policy;

- Privacy Policy; and
- Tenant Participation Strategy.

MONITORING AND REVIEW OF POLICY

Performance Monitoring

13.1 We report information request performance indicators in our Monthly Performance Report and a register of FOI/EICR requests received is available on our website.

13.2 Customer surveys will be carried out on a regular basis and the results of these surveys will be used to inform policy and service reviews. The tenants' newsletter will update tenants with how we have responded to survey feedback.

Review

13.3 We will review this policy every 4 years. More frequent reviews will be considered if, for example, there is a need to respond to new legislation, regulatory requirements, policy guidance, equality impacts or changes in good practice.

INTERPRETATIONS & ABBREVIATIONS

The following interpretation and abbreviations are used in this policy:

WORD	INTERPRETATION
HHP or Partnership	Hebridean Housing Partnership
Board	Means the Board of the Hebridean Housing Partnership
Board Members	All Members of the Board including co-opted Members
Data	Information which is: a) processed by computer or information planned to be processed by computer b) stored or collected for storage within a "relevant filing system"
Relevant Filing System	Information which is structured in such a way that specific personal data may be readily accessed.
Personal Data	Data about a living individual who can be identified from the data or any other readily obtainable information – this includes even basic information such as names and telephone numbers.
Special Category Data	Special category data is personal data that needs more protection because it is sensitive. It includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, and data concerning a person's sex life or sexual orientation. Information about criminal convictions and offences is subject to separate rules and safeguards under data protection law.
Data processing	Processing personal data means any operation carried out on personal data, whether by automated means or otherwise. This includes: • Obtaining • Recording • Holding

	• Organising • Adapting & altering • Retrieving • Consulting • Disclosing • Combining • Erasing • Blocking • Destroying References to "process" and "processed" shall be construed accordingly in this policy.
Commercially sensitive Data	Information, including personal data, the disclosure of which is likely to prejudice the legitimate commercial or business interests of the Partnership or another party. Whether information is commercially sensitive will depend on the circumstances and any applicable legal exemptions.
Data Controller	A person, company, or other body that determines the purpose and means of personal data processing.
AGM	Annual General Meeting
GDPR	General Data Protection Regulation. In this policy, references to GDPR should be read as referring to the UK GDPR unless otherwise stated.
FOISA	Freedom of Information (Scotland) Act 2002
EIR	Environmental Information (Scotland) Regulations 2004