

AGENDA ITEM 9iv

REPORT NO. VAL/15/16

Highland & Western Isles Valuation Joint Board

Data Protection Policy

10 June 2016

Document last saved: 27/05/16

Version	Changes	Author	Date
1.0	First release	F Finlayson	31/05/2016

HIGHLAND AND WESTERN ISLES VALUATION JOINT BOARD

DATA PROTECTION POLICY

1. Highland and Western Isles Valuation Joint Board (hereinafter referred to as “the Board”) supports the objectives of the Data Protection Act 1998, (hereinafter referred to as “the Act”) and intends to retain its present policy of maintaining the confidentiality of personal information processed automatically (on computers etc) and held on manual files which are considered to be “relevant filing systems” in terms of the Act.
2. The Board expects all elected members and employees to comply fully with this policy and the Data Protection Principles (Appendix).
3. The Assessor for the Board is registered with the Information Commissioners Office as a data controller. The register entry can be accessed at www.ico.org.uk . The registration number is Z5442561. The register entry will be reviewed annually.
4. The Board will hold the minimum personal information necessary to enable it to perform its functions, and the information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate and up-to-date, and that inaccuracies are corrected without unnecessary delay.
5. Personal information is confidential. Automated systems and relevant filing systems will be designed to comply with the Data Protection Principles. Personal information will be disclosed only where to do so is compatible with the Act and the details in the Data Protection Register.
6. It is the responsibility of the Assessor and Assistant Assessors to ensure compliance with this policy. All systems containing information about individuals must be identified, made secure, and notified to the Data Protection Officer for notification purposes. It is the responsibility of all employees to co-operate in this task. Upon discovering that the Board’s Policy on Data protection is not being complied with, the Clerk after consultation with the Treasurer of the Board, shall have full authority to take such immediate steps as considered necessary.
7. The Board will provide to any individual who requests it in the proper manner a written copy in clear language of the current information held. The Board may fix a fee for this service which in appropriate circumstances may be waived by the Clerk. Employees of the Board will not be required to pay any such fee when requesting access to information regarding their employment.
8. In cases where the Board provides services to outside organisations, no disclosure will be made without the written consent of the third party except under the direction of a Court Order checked by the Clerk.
9. All employees of the Board must comply with the requirements specified in the Highland Council’s Information Security Policy.
10. All employees will receive information security awareness training and will be vetted to basic level by Disclosure Scotland as part of the Board’s recruitment and induction process.
11. Disciplinary action may be taken against any Board employee for deliberate or reckless breach of any instructions contained in, or following from this Data Protection Policy.

APPENDIX

DATA PROTECTION ACT 1998

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed, fairly and lawfully and, in particular, shall not be processed unless:
 - at least one of the conditions in schedule 2 of the Act is met, and
 - in the case of sensitive personal data, at least one of the conditions in schedule 3 of the Act is also met.
2. Personal data shall be obtained for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with the purpose or those purposes.
3. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.