REPORT TO: **TAYSIDE VALUATION JOINT BOARD – 19 NOVEMBER 2018**

REPORT ON: **DATA PROTECTION**

REPORT BY: **ASSESSOR**

REPORT NO: **TVJB 23-2018**

1 PURPOSE OF REPORT

1.1 To update the Joint Board in relation to matters arising in respect of Data Protection and to seek approval of the updated Data Protection Policy and Data Security Breach Procedure.

2 RECOMMENDATIONS

2.1 The Joint Board is asked to note the content of this report and to approve the updated Data Protection Policy (Appendix 1) and the Data Security Breach Procedure (Appendix 2).

3 FINANCIAL IMPLICATIONS

3.1 Whilst the cost implications of process changes arising from the Data Protection Act 2018 and the related General Data Protection Regulations are minimal and will be contained within the existing Revenue Budget, the Joint Board is made aware that Data Protection failures can give rise to very significant fines of up to 20m Euro.

4 POLICY IMPLICATIONS

4.1 This report has been screened for any policy implications in respect of Sustainability, Strategic Environmental Assessment, Anti Poverty, Equality Impact Assessment and Risk Management. Risks attached to data protection failures are significant and include, amongst other things, potential fines. These risks are reflected within the Risk Management Strategy and Risk Register. There are no other major issues.

5 BACKGROUND

5.1 The Data Protection Act 2018 (the Act) has replaced the Data Protection Act 1998 and has given effect to the provisions of the General Data Protection Regulations EU 2016/679 (GDPR). The provisions of the Act and GDPR place a number of important responsibilities on the Assessor and Electoral Registration Officer and the Joint Board.

5.2 In the light of increased responsibilities arising in relation to data protection, the Data Protection Policy has been revised and this is attached as Appendix 1. In addition a dedicated Data Security Breach Procedure has been prepared and this is attached as Appendix 2.

5.3 Dundee City Council has agreed to its Data Protection Officer also acting as the Data Protection Officer for the Assessor and for the Joint Board. The contact details for the Data Protection Officer are contained within both the Data Protection Policy and the Data Security Breach procedure and are displayed on-line in the Board's Privacy Notice.

5.4 The Assistant Assessors for both Dundee and Angus Divisions have received GDPR Practitioner Certificate training to ensure that sufficient resource and knowledge is available within the organisation to deal with the day to day management of data protection issues.

5.5 In addition to the above, a number of other provisions have been put in place. These include:

- A revised Privacy Notice has been prepared and is now displayed on the Joint Board's website.
- Details of the Privacy Notice are now contained within emails, questionnaires and other communications routinely issued by the Assessor and staff.
- Scripts have been prepared which are now utilised by electoral registration staff to advise electors of their data protection rights when providing personal information by telephone.
- Revised Guidance Notes have been prepared for Staff.
- Staff have undertaken information security awareness training and this will be refreshed.
- A data audit has been undertaken and the results have been reflected in updated data retention and disposal policies.
- Several Data Sharing Agreements have been entered into with major organisations with which the Assessor and / or the Joint Board exchange personal data. A programme has been established to ensure that the implementation of data sharing agreements is extended to all appropriate organisations.

5.6 The Assessor's in-house Governance Group remains responsible for dealing with routine data protection issues on behalf of the Assessor and the Joint Board. The Group meets regularly and its proceedings are formally minuted, with minutes presented at meetings of the Assessor's Policy & Strategy Management Group for consideration as appropriate.

5.7 The Assessor will continue to report regularly to the Board on any issues arising in respect of Data Protection.

6 CONSULTATION

6.1 The Clerk and Treasurer to the Board have been consulted on this report.

7 BACKGROUND PAPERS

7.1 None.

ALASTAIR KIRKWOOD
Assessor

APPENDIX 1

TAYSIDE VALUATION JOINT BOARD

DATA PROTECTION POLICY

IMPLEMENTATION AND REVIEW

Responsibility for the implementation and annual review of this policy together with the communication of any resultant amendments across the Board and to relevant third parties is assigned to the Information Asset Owner (currently the Assessor).

Revision History

Version	Originator	Summary of Changes	Date
Original Document			29/09/05
v. 1	R Michalski	Item 6 – Replacement of Depute Assessor with Assistant Assessors	29/11/17
v 1.1	D Allan / A Kirkwood	Reviewed to conform to GDPR and the Data Protection Act 2018	16/10/18

Contents: **Page No.:**

1.0 Introduction

The Assessor and Electoral Registration Officer (the Assessor) and Tayside Valuation Joint Board (the Board) need to collect, store, process and, when required, share information or data about people in order to carry out their public functions and/or meet statutory obligations. This will include the personal data of a wide variety of individuals such as; council tax payers, ratepayers, past and present staff members, prospective staff members, suppliers of goods and services, etc.

Both the Assessor and the Board fully support the objectives of the Data Protection Act 2018, (hereinafter referred to as "the Act") and the General Data Protection Regulations (EU) 2016/679 (hereinafter referred to as "GDPR") and will maintain the confidentiality of personal data in accordance with these enactments.

The Assessor and the Board expect all elected members and employees to comply fully with this Policy.

This policy is not a stand alone document and should be read in conjunction with other related policies, procedures and guidance.

2.0 Purpose

The purpose of this policy is to ensure that the Assessor and the Board fully comply with their legal obligations as set out in the Act and GDPR in relation to the protection of personal data.

In complying with the Principles of Data Protection as laid down in the Act and the GDPR the Assessor and the Board may be held accountable by the Information Commissioner's Office (ICO), the body which oversees the data protection laws.

3.0 Roles & Responsibilities

It is the responsibility of the Assessor and Assistant Assessors to ensure compliance with this policy and 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 Assessor after consultation with the Data Protection Officer, shall have full authority to take such immediate steps as may be considered necessary.

Each member of staff who deals with personal data has a responsibility to follow all procedures and guidelines in relation to data protection in order to ensure that data is held securely, is not disclosed to any unauthorised parties, and that it is disposed of securely once it is no longer required to be kept.

This policy shall apply equally to any consultants, contractors, agents or any other individuals performing a function on behalf of the Assessor or the Board.

4.0 Personal Data

Personal data means any information relating to an identified or identifiable living individual who can be identified, directly or indirectly, in particular by reference to:

a) an identifier such as a name, an identification number, location data or an on-line identifier, or

b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

This includes the person's name, address, telephone number, national insurance number as well as any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

5.0 Special Category Personal Data

Special category personal data is data consisting of any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex life.
- Sexual orientation.

Special category personal data is subject to much stricter conditions of processing.

6.0 Data Controller Registration

The Assessor 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 Z6821924. The register entry will be reviewed annually.

7.0 Data Protection Principles

The Assessor and the Board require to ensure that all personal data is ingathered, held and disposed of in line with the following data protection principles. These principles require that all personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. 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.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. 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.

5. 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 General Data Protection Regulation in order to safeguard the rights and freedoms of the data subject.

6. 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

8.0 Data Protection Officer

The Assessor and the Board are required to have a named individual as the person with the overarching responsibility for ensuring compliance with the data protection principals and also to promote good practice throughout the organisation. The role of the Data Protection Officer (DPO) is to:

- Inform and advise the Assessor and the Board about their obligations to comply with the General Data Protection Regulation and other data protection laws.

- Monitor compliance with the General Data Protection Regulation and other data protection laws, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations and related audits.

- Provide advice about data protection impact assessments and monitor their performance;

- Co-operate with the supervisory authority (the Information Commissioner's Office).

- Act as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.

The Assessor and the Board have appointed Ian Smail, Information Governance Manager, of Dundee City Council to be the Data Protection Officer. The Data protection Officer can be contacted at:

Ian Smail
Information Governance Manager
Corporate Services
Dundee City Council
21 City Square
Dundee
DD1 3BY
Email: infogov@dundeecity.gov.uk(link sends e-mail),
Tel: 01382 434206

9.0 Data Security

The Assessor will ensure there are satisfactory arrangements in place for the security of special category data when held.

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.

- Personal information is not disclosed either orally or in writing or by any other means to any unauthorised third party.

All employees of the Board must comply with the requirements specified in the Board's e-mail/internet guidelines.

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.

Disciplinary action may be taken against any Board employee for deliberate or reckless breach of any instructions contained in this Data Protection Policy or other related documents.

10.0 Personal Data Breaches

The Act and GDPR introduce a duty on all organisations to report certain types of personal data breach to the ICO. This must be done within 72 hours of becoming aware of the breach. Staff are required to contact both their line manager and Assistant Assessor immediately on the discovery of a potential data breach in line with the Data Security Breach Procedure. In the absence of the Assistant Assessor any breach should be reported to the Assessor.

More information on breach management can be found on Information Commissioner's Office Guidance on Data Security Breach Management. Guidance on Data Security Breach Management

11.0 Retention of data

In order to comply with various legal requirements, the Assessor and the Board are required to retain data for differing lengths of time.

Once the data is no longer required to be held it must be securely destroyed. Information on the retention periods can be found in the Retention Guidelines & Disposal Arrangements and Schedule.

12.0 The rights of individuals

The Act and the GDPR provide individuals with the following rights regarding their personal information:

- The right to be informed about how their information will be used.
- The right of access to their personal information.
- The right to rectification, which is the right to require the Assessor or the Board to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Assessor or the Board where there is no longer a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Assessor or the Board processing their personal information.
- Rights in relation to automated decision making and profiling.

13.0 Lawful Processing

The Assessor and the Board must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual. The available bases are:

- **Consent:** the individual has given clear consent for the Assessor or the Board to process his/her personal data for a specific purpose.

- **Contract:** the processing is necessary for a contract that the Assessor or the Board has with the individual, or because the individual has asked the the Assessor or the Board to take specific steps before entering into a contract.

- **Legal obligation**: the processing is necessary for the Assessor or the Board to comply with the law (not including contractual obligations).

- **Vital interests:** the processing is necessary to protect someone's life.

- **Public interest:** the processing is necessary for the Assessor or the Board to perform a task in the public interest or in the exercise of official authority vested in the Assessor or the Board.

- **Legitimate interests:** the processing is necessary for the purposes of legitimate interests pursued by the Assessor or the Board or a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. However, this basis is not available to processing carried out by the Assessor or the Board in the performance of an official task: it can only apply to the Assessor or the Board is fulfilling a different role.

14.0 Processing

Processing for the purposes of data protection means everything from obtaining and gathering information to using the information and, eventually, destroying that information. Specifically, this includes:

- collection, recording, organisation or storage,
- adaptation or alteration,
- retrieval, consultation or use,
- disclosure by transmission, dissemination or otherwise by making available,
- alignment or combination, or
- restriction, erasure or destruction.

15.0 Data Sharing

The Assessor and the Board will only share personal data where this is permissible within the Act and the GDPR and is in line with the Data protection Principles.

The Assessor and the Board will provide free of charge to any individual who requests it in the proper manner, a written copy in clear language of their current personal information held.

The Assessor shall require any relevant parties who receive personal information to enter into a Data Sharing Agreement. The data sharing agreement will set out the lawful basis under which the data may be shared and other requirements relating to the manner in which the data may be processed and ultimately destroyed.

16.0 Other Policies, Procedures & Guidance

- Data Protection Security Breach procedure
- Disclosure of Information Policy
- Acceptable Use Policy for IT Systems
- Access Control Policy
- Data Access and Building Security Policy
- Procedure for Disposal of Media

- Government Security Classification, Handling & Disposal policy
- Security Incident & Weakness Policy
- Security of IT Systems – Guidance to Staff
- Security Policy
- Use of Cryptographic Techniques
- Remote & Mobile Working Policy
- E-mail & internet Guidelines
- Closed Circuit TV Policy

APPENDIX 2

TAYSIDE VALUATION JOINT BOARD

DATA SECURITY BREACH PROCEDURE

November 2018

IMPLEMENTATION AND REVIEW

Responsibility for the implementation and annual review of this policy together with the communication of any resultant amendments across the Board and to relevant third parties is assigned to the Information Asset Owner (currently the Assessor).

Revision History

Version	Originator	Summary of Changes	Date
Original Document	A Kirkwood		06/11/18

Overview
In terms of the Data Protection Act 2018 and the General Data protection Regulations, organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data. This procedure, which is based on the Information Commissioner's guidance on data security breach management, outlines what action should be taken in the event of a data security breach.

This Procedure applies to data breaches involving the Assessor and Electoral Registration Officer (hereinafter referred to as the Assessor) and Tayside Valuation Joint Board (hereinafter referred to as the Board).

A data security breach can happen for a number of reasons including:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- Blagging offence where information is obtained by deceiving the organisation who holds it

1. Reporting

All data security breaches or suspected data security breaches should be reported to both your line manager and Assistant Assessor immediately on the discovery of a potential data breach. In the absence of the Assistant Assessor any breach should be reported to the Assessor.

The Data Protection Officer (DPO) should immediately be informed by the Assistant Assessor or the Assessor of the breach or suspected breach.

The DPO currently appointed is **Ian Smail, Information Governance Manager, Corporate Services, Dundee City Council, 21 City Square, Dundee DD1 3BY Email: infogov@dundeecity.gov.uk(link sends e-mail) Tel: 01382 434206**

The Act and GDPR introduce a duty on all organisations to report certain types of personal data breach to the ICO. This must be done within 72 hours of becoming aware of the breach. More information on breach management can be found on Information Commissioner's Office Guidance on Data Security Breach Management.

2. Containment and Recovery

On discovery of a data security breach or suspected data security breach the Assistant Assessor or Assessor should:

1. Confirm the nature of the information lost, and in particular whether the information consists of sensitive personal data (medical information, details of convictions or alleged criminality etc.) or information of use in carrying out identity theft (such as bank account details).

2. Prevent any further loss of information and if possible any further dissemination of the information which has been lost or compromised.

3. Determine who needs to be made aware of the breach and what they need to do to contain the breach; this may include notifying affected individuals and reporting the loss to the Information Commissioner.

3. Assessing the Risks

The Assistant Assessor or Assessor will determine the risks associated with the loss.

The risks associated will be dependent on:

- The type of data involved
- How sensitive the information is
- Whether there were any protections in place, e.g. encryption of a portable device
- What has happened to the data, if known.
- How many individuals' personal data are affected by the breach.
- What harm can come to those individuals whose data has been lost.
- Whether there are any wider consequences to the loss of the data.
- If individual's bank details have been lost, consideration will be given to contacting the banks for advice on preventing fraudulent use.

The assessment will be immediately communicated to the Assessor Assessor and the DPO

4. Notification of breach

Informing people and organisations that the Assessor or the Board has experienced a data security breach is an important part of this breach management procedure.

Consideration will be given to:

- Who will be notified (police, banks etc),
- What we will be notifying them of, and
- How we are going to notify them.

If a decision is taken to notify individuals of the breach, the notification will tell them how and when the breach occurred and what data was involved. The notification will also tell the individual what has and is being done by the Assessor and the Board to respond to the breach. The decision to notify individuals will normally be taken by the Assessor or

Assistant Assessor. Decisions on notifying the Information Commissioner will be taken by the DPO in conjunction with the Assessor or Assistant Assessor.

If the Information Commissioner requires to be notified, the DPO will do this as soon as possible following notification of the breach but certainly within 72 hours via the following link: https://ico.org.uk/for-organisations/report-a-breach/

5. Evaluation and response

Part of the overall breach response will be to investigate the causes of the breach and also the effectiveness of the Assessor's response to the breach.

Simply containing the breach is not acceptable, particularly if the breach was caused (even in part) by a systematic or ongoing problem. Action must be taken to rectify the underlying problem. A review will be conducted by the Assistant Assessor and reported to the Management Team. A report on the review must be made available to the Assessor and DPO within three weeks of the incident and must address issues which caused the incident and make recommendations as to the steps necessary to prevent or minimise such an incident recuring.

Based on "lessons learned" policies and procedures will be reviewed and updated if required.

Any data loss reported to the Information Commissioner will be reported to the next meeting of the Management Team.