DATA PROTECTION POLICY

Title	Data Protection Policy
Who should use this	All Staff
Author	SAC/Adapted by AVJB
Approved by Management Team	22 August 2018
Approved by Joint Board	
Reviewer	**Assessor & ERO/HOVS**
Review Date	**2021**

Review History

REVIEW NO.	DETAILS	RELEASE DATE
1	UPDATED TO REFLECT GDPR REGULATIONS 2016	JULY 2018
2		
3		
4		
5		

Policy Statement

The objective of data protection is to ensure that the rights and freedoms of data subjects are considered in the collection and processing of personal data.

The purpose of this policy is to ensure that the personal data collected and processed by Ayrshire Valuation Joint Board ('the Board') is managed in accordance with the General Data Protection Regulation 2016 and other Data Protection legislation.

This policy applies to all staff of the Board. Other agencies and individuals working with the Board who have access to personal information held by the Board are also required to comply with this policy.

CONTENTS

1. Introduction

The purpose of Data Protection law is to protect the personal data rights and privacy of living individuals. The Board is required to demonstrate to the Information Commissioner (UK Regulator of Data Protection law) that they are fully compliant with the General Data Protection Regulation 2016 (GDPR) and has incorporated the concept of 'Privacy by design' into its routine processes and procedures. The Board must also guarantee that it has adequate mechanisms in place to prevent against unauthorised or unlawful processing and accidental loss, damage or destruction of personal data.

In the course of its everyday business, the Board collects and processes personal information relating to Ayrshire residents, current, past and prospective employees, suppliers, clients and others with whom it communicates. In addition, it may occasionally be required to collect and disseminate certain types of personal information to comply with the statutory requirements of government departments for business purposes. Given the operational importance and sensitivity of such data, it is essential that such information is managed and processed in an efficient and systematic manner to ensure the Board is not only compliant but can demonstrate our adherence to the six principles of GDPR (please see section 3 of this policy document).

To ensure best practice and full compliance with Data Protection law, Ayrshire Valuation Joint Board has access to the support and guidance of the South Ayrshire Council Information Governance Team, based within Regulatory Services to advise and assist the Board. The Democratic Governance Manager is the named Data Protection Officer for Ayrshire Valuation Joint Board. The Assessor & ERO for Ayrshire Valuation Joint Board is registered with the Information Commissioner as a data controller.

This policy will be reviewed bi-annually and may be altered at any time as appropriate.

2. Definitions

Personal Data

'Personal data' means any information relating to an identified or identifiable living person ('data subject' see below).

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data Subject

Data subject means 'an individual who is the subject of personal data'. A data subject must be a living individual.

Data Controller

Data controller is defined as ‘a person (organisation) who (either jointly or in common with other persons) determines the purposes for which, or the manner in which, any personal data are, or are to be, processed’.

Data Processor

The data processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Information Asset Register

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and used efficiently to help the Board provide a service. Information assets have recognisable and manageable value, risk, content and lifecycles. Maintaining an Information Asset Register (IAR) is a requirement of the GDPR. The IAR is a simple way to help Board Officers understand and manage the Board’s information assets and the risks around those assets.

The Board’s IAR includes the following information:

- Identification of each information asset
- Where our information is held
- Why we keep it
- Who is allowed to access it
- How long we keep it
- How we destroy it

Processing

The definition of processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Category Data

This is personal data consisting of information relating to 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. Personal data relating to criminal convictions and offences are not included within special category data per se but similar extra safeguards apply to its processing.

Record

A record is recorded information, in any form, including data in systems created, received and maintained by Ayrshire Valuation Joint Board and kept as evidence of such activity.

Vital Record

This is a record without which an organisation would be unable to function or to prove that a key activity had taken place.

Format

A record can be in any format including (but not limited to) paper files, e-mail, audio/visual, electronic documents, systems data, databases, digital images and photographs.

Records Management

Is the control of Ayrshire Valuation Joint Board's records during their lifetime, from creation to storage until archiving or destruction.

3. Principles of Data Protection

There are six data protection principles which the Board as a Data Controller is required to comply with. Personal data must be:

Principle 1 - Processed lawfully, fairly and in a transparent manner

The Board must have lawful authority for processing personal information and the purpose of the processing must be explained to the data subject. This links to the right of a data subject to be informed. This is achieved by providing data subjects with Privacy Notices (please see section 8 of this policy document). Any sharing of personal data with other organisations will be appropriately documented in the Privacy Notice.

Principle 2 – Obtained for specific, explicit and legitimate purposes

The Board must ensure that personal information is not processed for a purpose which is incompatible with the purpose for which it was collected. Processing must fall strictly within the purposes for which the data were obtained. Where the Board is obliged to obtain personal data for a statutory purpose, the data may not be processed for any other statutory purpose unless it directly relates to the original purpose.

It should be noted, 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.

Principle 3 – Adequate, Relevant and limited to what is necessary

Personal information must be adequate relevant and limited to collecting only what is needed to get the job done given the purposes for which it is held. This will depend on circumstances, however care should be taken to ensure that information is not collected 'just in case' and that files are checked regularly to ensure that unnecessary information is removed.

Principle 4 – Accurate and where necessary kept up to date

Personal data must be accurate and up to date. Where it is discovered that information that is held by the Board is inaccurate, the error must be rectified immediately.

Principle 5 – Kept in a form that permits identification of data subjects and held for only as long as necessary

Personal data must be kept in a manner that allows data subjects to access it under a subject access request (please see section 7 of this policy document).Personal data must not be kept for longer than necessary for the purpose it was collected. The Board's Records Retention Schedule must be applied at all times.

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 in order to safeguard the rights and freedoms of the data subject.

Principle 6 – Held securely

Appropriate security measures must be taken against unauthorised processing and against accidental loss, destruction, theft, or damage of personal data**.** Managers must therefore scrutinise their record keeping at all levels to ensure that appropriate security is in place.

If any information is processed on behalf of the Board by a third party, written contracts must be in place in terms of which the third party processor can act only on the Board's instructions and must comply in full with the security obligations which are imposed on the Board.

Where personal data has to be taken off-site, this will be restricted to only what is necessary to undertake the required task. The data must be kept secure at all times.
To help adhere to the above principles, the Board will ensure that:

i. all staff are aware of their specific responsibilities under the Data Protection law through policies and procedures which can be readily accessed via SharePoint;

ii. the Assessor & ERO will be responsible to maintaining the Information Asset Register (IAR) to ensure it is accurate and kept up to date.

iii. a regular review and audit of the way personal information is managed and processed to ensure best practice and compliance with the law is conducted;

iv. staff managing and handling personal information receive appropriate training and supervision; and

v. all enquiries from data subjects wanting more information about how the Board handles their personal information are directed to the appropriate person and that any such enquiries are dealt with promptly and courteously.

4. Roles and Responsibilities

Overall responsibility and accountability for ensuring that all staff and associated third parties comply with data protection legislation, this Policy and associated policies and procedures, lies with the Assessor & Electoral Registration Officer.

Data Controller

The Assessor & ERO, in addition to being a Data Controller in her own right has responsibility for the information held by Ayrshire Valuation Joint Board.

Senior Information Risk Owner

The Head of Valuation Services and Assistant ERO is the Senior Information Risk Owner (SIRO) and has overall strategic responsibility for governance in relation to data protection risks. The SIRO:

- Acts as advocate for information risk at the Senior Management Team.
- Oversees culture change regarding information risks in a realistic and effective manner.
- Oversees the reporting and management of information incidents.
- Ensures the Information Asset Owner roles are in place to support the SIRO role.

Management Team

Their role is to understand what information is held by the Board, what is added and what is removed, how information is moved, and who has access and why. They must ensure that written procedures are in place and followed relating to these activities, risks are assessed, mitigated and the risk assessment processes are audited. They are also responsible for ensuring the IAR entries are accurate and kept up to date.

Data Protection Officer

The role of the Data Protection Officer (DPO) is to:

- Inform and advise the Board and its employees 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 Information Commissioner's Office (ICO).

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

The Board's DPO is South Ayrshire Council's Democratic Governance Manager.

Records Manager

The Records Manager is responsible for developing, delivering and maintaining a comprehensive information governance and security framework for the Board. He will help ensure compliance with legislative frameworks governing the access to, retention, sharing and disposal of information.

He will collect information to identify the Board's processing activities, analyse the processing activities and provide information to the DPO so she can inform, advise and issue recommendations to the Board.

He will assist services in the carrying out of data protection impact assessments (DPIA), where required.

The Board's Record Manager is the Head of Valuation Service and Assistant ERO.

Individual Members of Staff

Individual members of staff are responsible for protecting personal information held or processed on computer, or held in paper records, within their care. They also have the responsibility to report any breach or potential breach immediately to their line (please see section 9 of this policy document).

5. Lawful basis for processing

The lawful basis for processing (using) personal data are set out in the GDPR. At least one of these must apply whenever the Board processes personal information:

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

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

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

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

If the Board is processing special category data or criminal conviction data then they must consider further special conditions for processing.

6. Rights of Data Subjects

The GDPR provides data subjects 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 (subject access request)
- The right to rectification, which is the right to require the Board to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Board where the Board no longer has 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 Board processing their personal information.
- Rights in relation to automated decision making and profiling.

The legal basis for processing information determines what rights are applicable. Further information on data subjects' rights can be found at www.ico.org.uk. Data subjects rights are also contained in the Privacy Notices.

7. Subject Access Requests

Data subjects have the right to request information which is held about themselves. The Board has a process for handling subject access requests, the relevant guidance can be found on SharePoint. The public can also access this information via our website www.ayrshire-vjb.gov.uk.

8. Privacy Notices

Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. The Board must provide data subjects with information including: our purposes for processing their personal data, our retention periods for that personal data, and with whom it will be shared within a 'Privacy Notice'.

Privacy Notices must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. To meet this requirement the Board will adopt a combination of different techniques including layering, leaflets, and our website to inform our residents on how we use their personal data.

9. Breaches

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Despite the security measures taken to protect personal data held by the Board, a breach may occur.

The Board has a legal requirement to notify the ICO within **72 hours** of any personal data breach where it is likely to result in a risk to the rights and freedoms of data subjects. Failure to notify the ICO may result in a significant fine being imposed.

It is the Assessor & ERO's or the Head of Valuation Services & Assistant ERO's responsibility to assess each personal data breach for consideration to report to the ICO. The Assessor & ERO or the Head of Valuation Services & Assistant ERO also has a duty to report any personal data breach to any affected data subjects. Therefore it is imperative all personal data breaches, both suspected, and confirmed, are reported immediately.

Appropriate steps should be taken to remind contractors and third party users of Board information systems of:

- their legal obligation to report personal data breaches as per the GDPR
- their contractual obligations, where applicable
- in all other cases; encourage support of good practice, as outlined above.

Contract owners must ensure that when contracts are negotiated or renewed they contain appropriate obligations to support this procedure. Support is available from the Board's procurement and legal advisers.

Where an incident involves the loss of ICT equipment or functionality, the event should also be logged with the Board's Principal Administrative Officer and the Business Support and Development Officer:

10. Notification

The Board must advise the Information Commissioner's Office that it holds personal information about living people. It must also pay a fee in accordance with the Data Protection (Charges and Information) Regulations 2018.

11. Data sharing

The Act does not prohibit the sharing of personal data where it is appropriate. All sharing of data with other organisations must be appropriately documented and a Data Sharing Agreement in place before any data is shared.

12. Related policies and Procedures

Records Management Policy.
Information Security and ICT Acceptable Use Policies.
Records Retention Schedule.
Freedom of Information Policy.
Complaints Handling Procedure.
Data Protection Sheet for Employees.

13. Further Information and Guidance

Ayrshire Valuation Joint Board
9 Wellington Square
Ayr
KA7 1HL
E-mail: assessor@ayrshire-vjb.gov.uk
Tel: 01292 612221

Further information is also available from the Information Commissioner's website - www.ico.org.uk.