DATA PROTECTION BREACH PROCEDURE

Title	Data Protection Breach Procedure
Who should use this	All Staff
Author	SAC/Adapted by AVJB
Approved by Management Team	21 August 2018
Approved by Joint Board	N/A
Reviewer	**Assessor & ERO**
Review Date	**2020**

Review History

REVIEW NO.	DETAILS	RELEASE DATE
1	NEW	JULY 2018
2		
3		
4.		

1 Scope of Procedure

This procedure covers all information and related facilities owned by Ayrshire Valuation Joint Board.

2 Purpose of Procedure

The purpose of the procedure is to standardise our response to any reported breach or loss of information. Ensuring all incidents are logged and managed in accordance with our legal obligations imposed by Data Protection legislation.

3 Definitions

Data Protection Breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Data Protection Officer (DPO) –a statutory post created under the General Data Protection Regulation 2016 (GDPR) responsible for providing advice on data protection legislation and monitoring compliance. The Board's DPO is the Democratic and Governance Manager, Legal & Democratic Services, South Ayrshire Council.

Personal Data – any information relating to an identified or identifiable living individual, for example – name, national insurance number, date of birth.

4 Aim of Procedure

By adopting a standardised consistent approach we will ensure:

- All incidents are reported as soon as practicable to any notifiable external agencies. These may include the Information Commissioner's Office and Police Scotland.
- Impact of incidents is fully understood and action is taken to prevent or limit further breaches/damage
- All incidents are recorded, logged and investigated in a form that will withstand internal and external scrutiny
- All incidents are reported as soon as practicable to allow consideration by the DPO to notify the affected individuals of a data protection breach
- Incidents are reviewed to identify improvements in policy, procedure or training.

5 Responsibilities for applying and managing this procedure

Everyone who handles information, be it paper records, hard copy or electronic, within the Board has a responsibility to ensure the safekeeping of that information and to comply with this procedure.

Head of Valuation Services & Assistant ERO and Line Managers are responsible for ensuring all users are aware of this procedure and comply with its terms.

The Head of Valuation Services & Assistant ERO will offer advice to staff on how to respond to and manage data protection breaches.

Contact details can be found at section 7 of this guide.

The Assessor & ERO or the Head of Valuation Services & Assistant ERO will report significant breaches/incidents all relevant parties and will make recommendations on appropriate remedial steps to the Management Team.

6 Examples of data protection breach and other security incidents

Examples of a data protection breach include:

- Disclosing personal information to parties not requiring to have access to it, for example – sharing a Council Tax Payers details with another service or third party when there is no requirement

- Leaving files containing personal data in view of unauthorised persons, for example – going home leaving a personnel record on your desk in plain view where anybody could read it

- Accessing a person's record inappropriately, for example - viewing elector details of neighbours, friends etc.

- 'A major incident causing a loss of availability of ICT systems'

- Sending an email containing personal information to the wrong recipient

- Giving out personal information over the telephone to or within earshot of unauthorised individuals, for example – giving out personal information without confirming the person you are speaking to has the right to receive that information and is who they claim to be

- Positioning of PC screens where sensitive information could be viewed by the public

- Storing personal information on unencrypted laptops

- Inadequate disposal of confidential material containing personal information

7 Reporting information security incidents and data breaches

All incidents both suspected and confirmed should be reported immediately.

By emailing –The Head of Valuation Services & Assistant ERO. Please put '**Data Breach'** in the subject heading and use the form in appendix one.

If you are in any doubt seek help and advice from the Head of Valuation Services & Assistant ERO or your Line Manager as a matter of urgency.

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.

Contractors and Third Party Users

Steps must also 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 General Data Protection Regulation 2016
- their contractual obligations, where applicable
- in all other cases encourage support of good practice, as outlined above.

Where relevant, all staff must ensure that when contracts are negotiated or renewed they contain appropriate obligations to support this procedure. Support is available from South Ayrshire Council's procurement and legal teams.

8. Breach Management Plan

The Head of Valuation Services & Assistant ERO will in the first instance investigate all data breaches using the Information Commissioner's Office (ICO) suggested Breach Management Plan:

1. Containment and recovery.
2. Assessment of ongoing risk.
3. Notification of breach.
4. Evaluation and response.

1. Containment and Recovery.

Containment and recovery involves limiting the scope and impact of the data breach as quickly as possible The affected service will report directly to Head of Valuation Services & Assistant ERO who will be responsible for reporting to the DPO.

Steps **might** include: -

- Attempting to recover any lost equipment or personal information.
- Shutting down an IT system.
- Contacting the South Ayrshire Council Communications Team so they can be prepared to handle any press enquiries or to make any press releases.
- The use of back-ups to restore lost, damaged or stolen information.

- If bank details have been lost/stolen consider contacting banks directly for advice on preventing fraudulent use.

- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

- An identification of any applicable ICT or business continuity plans which document the business tolerance to disruption for the unit(s) impacted by the incident.

2. Assessment of ongoing risk.

The initial investigation should be completed urgently and wherever possible within **24 hours** of the breach being discovered/reported. Staff may be directed to gather evidence or submit statements to the Head of Valuation Services & Assistant ERO. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

The Head of Valuation Services & Assistant ERO will ascertain whose information was involved in the breach, the potential effect on the data subjects and what further steps are required to remedy the situation. The following are the categories of information that may need to be considered:

- The sensitivity of the personal information.

- How many individuals are affected by the breach?

- What protections are in place (for example, encryption)?

- What happened to the information?

- Whether the information could be put to any illegal or inappropriate use.

- What could the information tell a third party about the individual?

3. Notification of Breach.

Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions. Notifications of data protection breaches will be the responsibility of the Assessor & ERO or the Head of Valuation Services & Assistant ERO.

Any other incident not breaching data protection but deemed a security incident will fall under the remit of the Head of Valuation Services & Assistant ERO to determine the requirements of notification.

There may be occasions whereby Police Scotland require to be notified where there is suspected criminal activity. The decision to contact the Police Scotland will lie with the Assessor & ERO or the Head of Valuation Services & Assistant ERO taking advice from the DPO.

Personal Data Breaches

We have 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 individuals. Failure to notify the ICO could 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 individuals. Therefore it is imperative all personal data breaches both suspected and confirmed are reported immediately as per the procedure described above.

Other bodies

There may be occasions whereby we are required to inform other governing bodies, partnership agencies or other stakeholders of an information security incident. Notification of any other body will be on the advice of the DPO, the Assessor & ERO, Head of Valuation Services & Assistant ERO, and/or the Management Team.

4. Evaluation and response.

Once the DPO has evaluated the effectiveness of the Board's response to the breach and completed a full investigation as to the cause. Recommendations may be made to the Board to make relevant changes to mitigate the chance of any reoccurrence of a breach.

9. Legislation

The Board has an obligation to abide by all relevant UK and European legislation. The legislation that applies includes but are not limited to: -

General Data Protection Regulation 2016
The Data Protection Act 2018
And any subsequent amendments or modifications to UKData Protection legislation.

10. Appendices

Appendix 1 – Data Protection Breach - Incident Reporting Form

Appendix 1 – Data Protection Breach Incident Reporting Form

Data Breach Reporting Form

Please use this form to report any form of Data Breach.

The Head of Valuation Services & Assistant ERO will be in touch

Did you identify the breach or are you reporting on someone else's behalf?

I Identified the Breach ☐ **I am reporting on someone else's behalf ☐**

Who is reporting the breach? Please provide Contact Details:

Name	
Email Address	
Telephone	
Section	

Who found the breach:

Name	
Email Address	
Telephone	
Section	

Time and Date Breach identified: Click here to enter a date.

Description of the Data breach:

What happened? Cause of breach?

Description of the personal data affected?

For example name, address, bank details, etc.:

For AVJB Investigating Team Use Only:	
Volume of data involved:	
Is the breach contained or on-going?	
If on-going what actions are being taken to recover data or minimise damage?	
If the data was lost / stolen, were there any protections in place to prevent access/misuse? *For example - encryption*	
Who has been informed of the breach?	
Any other relevant information:	

Submit

Email to assessor@ayrshire-vjb.gov.uk

Received by	
Time and date	