ANGUS COUNCIL

DATA PROTECTION BREACH RESPONSE PLAN

Version:	V01.5
Author:	Angela Dunlop, Team Leader – Information Governance
Date of Approval:	16 January 2020
Approved by:	Information Governance Working Group
Date issued:	16 January 2020
Next review date:	12 April 2023
Related Documents	DP Breach Checklist template

Document Control Sheet

Author(s): Angela Dunlop, Team Leader – Information Governance

Document Title: Data Protection Breach Response Plan

Review/Approval History

Date	Name	Position	Version Approved	Date Approved

Version	Date	Brief Summary of Changes	Author
1.1	January 2018	Initial Draft	Anne Garness
1.2	March 2018	Amendments	Anne Garness
1.3	July 2018	Checklist now separate template document. Notification that DP intranet page not available – under review	Cath Bowman
1.4	February 2019	Updated link to ICO form in Appendix 1	Cath Bowman
1.5	February 2019	Amendments approved by IGWG	Angela Dunlop
1.5	January 2020	Checked for accuracy	Angela Dunlop
1.5	October 2021	Checked for accuracy	Angela Dunlop
1.5	April 2022	Links updated and checked for accuracy	Angela Dunlop
1.6	February 2024	Brief changes and links updated for accuracy	Claire McBean

Contents:

Part 1 Steps taken to prevent breaches
Part 2 What to do in event of a breach

Flowchart: Reporting a Breach in Data Protection
Step 1 Notification to Data Protection Officer
Step 2 Investigation by Information Officer
Step 3 Data Protection Officer Determination
Step 4 Notification to Information Commissioner's Office and other relevant persons
Step 5 Take Action

Additional resources:

- Breach Checklist
- List of Senior Information Officers (SIOs) and Information Officers (IOs)
- E learning module
  Log In using the above link

ANGUS COUNCIL

DATA PROTECTION BREACH RESPONSE PLAN

PURPOSE

The purpose of this plan is to have effective procedures in place to deal with potential security incidents compliant with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

It should be noted that a breach will not just oblige the council to carry out an investigation but also to implement recovery procedures including, where necessary, damage limitation measures.

Part 1 of the plan sets out the steps the council has taken to prevent breaches and Part 2 of the plan sets out the steps to be followed when it is thought there has been a data breach.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

PART 1

Steps taken to prevent breaches:

1. The council has in place an Information Governance framework with an Information Governance Steering Group (IGSG) led by the council's Chief Information Governance Officer (CIGO) and comprising of Senior Information Officers (SIOs) representing services across the council as well as Angus Health & Social Care Partnership (AHSCP) and ANGUSalive. This group has strategic responsibility for data protection and oversees the Information Governance Working Group (IGWG). The IGWG comprises of Information Officers (IO) for each service as well as AHSCP and ANGUSalive representatives, who have responsibility for information governance matters within their service, including compliance with data protection rules.

2. Policies and procedures for breach prevention have been put in place and can be found on the Information Governance webpage.

3. Contractual conditions have been revised in light of GDPR to be compliant with the responsibilities of data processors and collaboration with Tayside Procurement Consortium (TPC) has taken place to ensure TPC contracts are also compliant. The council's standard Service Level Agreement has also been reviewed.

4. All staff and members must complete an induction Data Protection E-learning course when they start employment with the council and thereafter a mandatory annual Data Protection E learning module which is reviewed annually.

5. Statistics from the data breach register are circulated regularly to SIOs and IOs.

PART 2

Steps to be taken in event of possible breach:

Under the GDPR, the council is obliged to notify the Information Commissioner's Office (ICO) of breaches which have a risk of affecting the rights and freedoms of individuals within 72 hours of being made aware of it. It is therefore essential that all staff are aware that breaches need to be brought to the attention of IOs and Managers straight away. The purpose of immediate notification is to encourage data controllers (i.e., the council) to act promptly, contain the breach and if possible, recover the personal data.

Oops! We've had a breach

Examples of our breaches……Don't let it happen to you!

- Wrong address on letters to staff/clients
- Emailing wrong member of staff (this is a breach if personal information sent)
- Wrong attachments being sent out either by email or hardcopy mail
- Lost unencrypted memory stick
- File saved on incorrect part of server (again this is a breach if personal information shared)
- Filing left behind in vacant office
- Staff not using secure print

Reporting A Breach In Data Protection

*Oops! We've noticed a breach

72 hours start ticking

Alert an Information Officer (IO) within your directorate

Is there any immediate action we need to take to stop this getting worse

No

Yes

Do it

IO tells our Data Protection Officer (DPO) (or agreed Officer) and starts investigation

IO and DPO (or agreed Officer) look at the information and makes a judgement whether it needs reporting to the Information Commissioner's Office (ICO)

Have rights and freedoms of individuals been affected?

No

Yes

Take action to make sure it does not happen again

Notify ICO and other relevant people**

Record breach/Share learning

72 hours is up

Await decision

Hear and accept penalty imposed. This could be a fine or even a criminal charge!

*a breach in data protection is when we have lost, shared or someone else has found personal data that we should have kept safe and secure

**we may need to tell: the person or people affected, other departments and maybe even the police

STEP 1- NOTIFICATION TO DATA PROTECTION OFFICER

1. As soon as a member of staff becomes aware of a security incident or possible breach, they should intimate this to their service IO and their Manager. The IO must intimate the occurrence of a security incident to the Information Governance Team InformationGovernance@angus.gov.uk who, in the event of a serious breach, will immediately notify the council's Data Protection Officer (the DPO). It is important to provide as much information as possible to allow the Info Gov team time to review details. The 72-hour clock starts ticking the minute the council is notified of the breach. **(See Step 4).**

2. There are three types of data protection breaches: -

   "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
   "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
   "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

STEP 2 – INVESTIGATION BY IO

1. The IO must carry out an urgent investigation to establish the facts so that an informed decision can be made as to whether rights and freedoms have been breached and if ICO notification is required. Completing the **breach checklist** is a useful guide as it identifies the facts that need to be established. This should be completed by the member of staff who was responsible for the breach and the service IO as a matter of urgency.

2. The IO should check any relevant Data Privacy Impact Assessment which may assist in determining the effect of the breach on the person whose information has been lost, disclosed etc.

3. The IO must also check any arrangements with processors (contractors) if they have been involved in the incident. Check the contract conditions – they should require the processors to provide assistance to the council. The contract conditions should also require a processor to intimate any breach to the council immediately so that the council is able to comply with their obligation to notify the ICO within 72 hours.

4. Once the initial investigation is complete, IOs should pass the checklist and available evidence to informationgovernance@angus.gov.uk (InfoGov mailbox) to ascertain whether the completion of the ICO notification form is required.

5. It is understood that it may not be possible to collate all the information immediately but a referral to the ICO must be made within 72 hours of the council being aware of a referable breaches and therefore, the initial investigation must be concluded and referred to the InfoGov mailbox straight away. Thereafter the investigation can be continued as required and further information provided to the InfoGov mailbox when known.

STEP 3 – DPO DETERMINATION

If InfoGov/IO has deemed the breach high risk, they will pass the checklist and evidence to the DPO. The DPO will consider the completed notification/checklist form/report and assess whether the rights and freedoms of an individual have been breached and if ICO notification is required. An objective assessment of the risk is required. Consideration of the likelihood and severity of the risk and circumstances are required e.g., take into account the special characteristics of the individual.

STEP 4 – NOTIFICATION TO ICO AND OTHER RELEVANT PERSONS

1. ICO

If the DPO determines that there has been a risk to the individual's rights and freedoms, and determines reasons for reporting, instructions will be given to the IO to create a notification form to be sent to the ICO.

This notification form should be checked by the DPO before submission. As a minimum, the following information must be provided: -

- Description of nature of the breach i.e., categories of individual/information and numbers affected
- Name and contact details of DPO
- Likely consequences of breach
- Description of measures taken

Notification to the ICO can be carried out in phases if it is not possible to collate all the information within the 72-hour period. If it is not possible to notify within 72 hours, then reasons for the delay must be provided.

2. DATA SUBJECT

Urgent consideration must be given as to whether the data subject should be informed. Notification is only required where there is a high risk to the individual's rights and freedoms. Therefore, the threshold is higher for intimation to individuals than it is for notification to the ICO. Such intimation must be made as soon as reasonably feasible.

The DPO and IO will decide on the best means of contacting the individual.

The following information should be provided to the individual: -

- Description of nature of breach
- Name and contact details of DPO
- Description of likely consequences of breach
- Description of measures taken.
- Advice to help the individual protect themselves from effects of the breach where appropriate

Individuals should also be advised of their right to refer the matter to the ICO where they are not satisfied with the council's response to the breach. How to contact the ICO

3. POLICE

A data breach could be deemed a criminal offence, for example a cyber-attack. The DPO will determine if the matter needs to be referred to Police Scotland.

4. HUMAN RESOURCES

The IO should consult with Human Resources to see if disciplinary action is appropriate.

STEP 5 – TAKE ACTION

1. The IO will agree with the DPO and liaise with other services, as appropriate, on the immediate steps, if any, required to ensure damage limitation e.g., recovery action by IT. It may be that urgent action must be taken whilst the investigation is ongoing **(See Step 2).**

2. Having considered all the facts the IO shall agree with the DPO what remedial measures are necessary e.g., review of existing policies or procedures/new policies or procedures or if additional or modified training is required. An action plan will be put in place where it is deemed necessary by the IO and implementation overseen by the SIO.

STEP 6 – ICO DETERMINATION

1. IO to review the ICO response and agree an action plan with the SIO taking into account any ICO recommended actions **(See Step 5)**.

STEP 7 – REGISTER

1. InfoGov will complete the council's register of breaches. The council is required to maintain a register with details of the breach, effects and consequences, remedial action and reasoning for decisions taken. This register is kept on the Information Governance SharePoint site.

Further guidance on data protection breaches is available at ICO guidance.