ANGUS COUNCIL

DATA PROTECTION BREACH RESPONSE PLAN

Version:	V01.5
Author:	Angela Dunlop, Team Leader – Information Governance
Date of Approval:	21 March 2019
Approved by:	Information Governance Working Group
Date issued:	21 March 2019
Next review date:	21 March 2020
Related Documents	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

Contents:

Additional resources:

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

  Type "Data Protection" in the search bar

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).

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 Senior Information Officers (SIOs) representing services, Manager Governance, Risk & Scrutiny, Service Leader – Digital Enablement & IT, Team Leader - Information Governance, the council's Data Protection Officer (DPO) and representatives from ANGUSalive and the Angus Health & Social Care Partnership (AH&SCP). This group has strategic responsibility for Data Protection and oversees the Information Governance Working Group (IGWG). This group comprises Information Officers (IO) for each service and AH&SCP 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 eg physical files policy.

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. A communications strategy has been developed to ensure that staff, members, contractors and service users are made aware of GDPR and its implications for them.

5. A training plan is in place. All staff and members must complete an E learning module which informs them of GDPR. Awareness raising of the data breach response plan has been provided to IOs.
6. Entries onto the data breach register are circulated to all SIOs and IOs as a means of sharing lessons learnt and to improve awareness of breaches and best practice.

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 so it is important that all staff are aware that breaches need to be brought to the attention of IOs straight away. The purpose of immediate notification is to encourage data controllers (ie the council) to act promptly, contain the breach and if possible, recover the personal data.

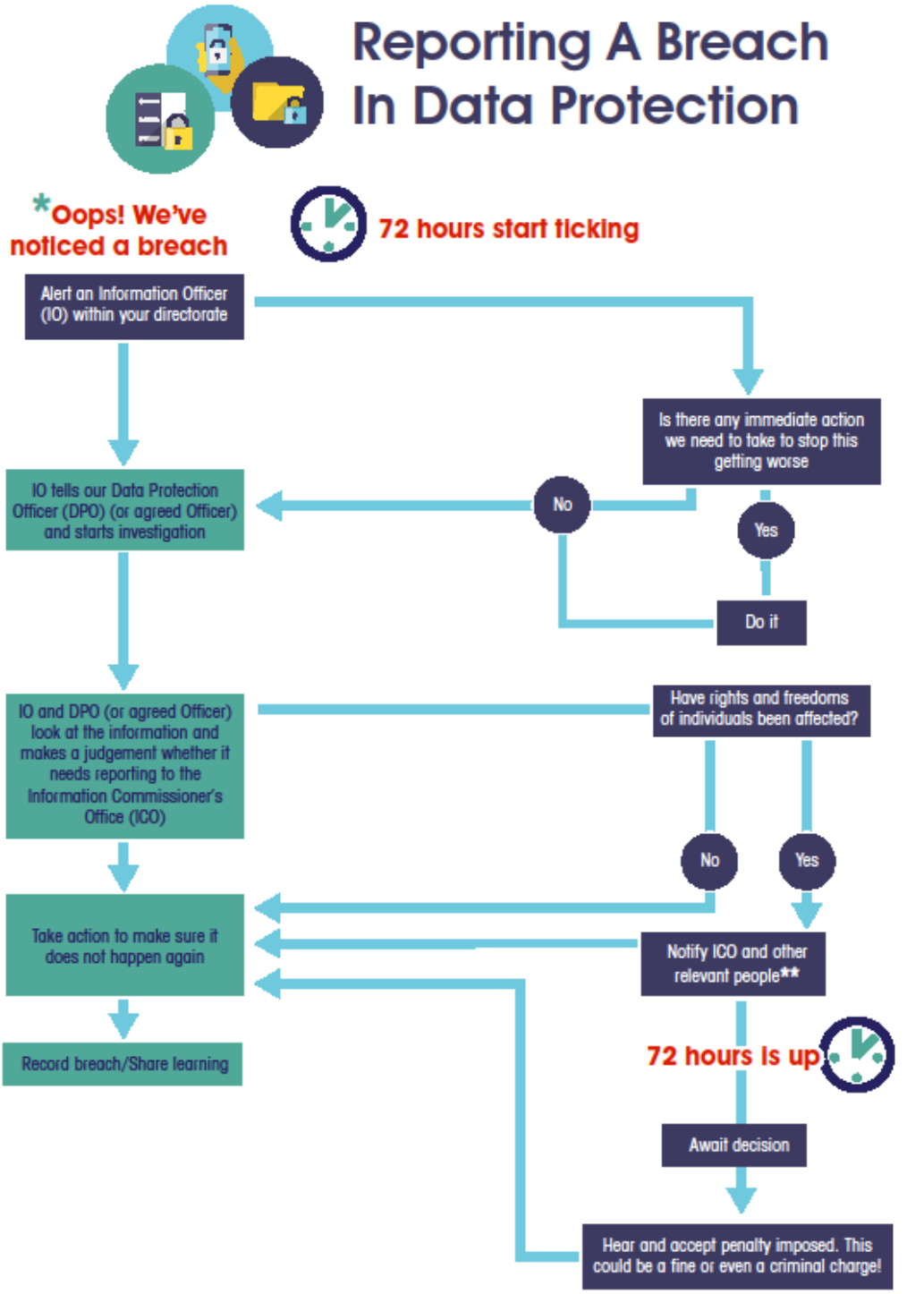
Where a breach has been intimated to the council by way of a complaint this should be dealt with in the normal manner i.e. in line with the council's complaints process but in addition complainers should be advised of their right to raise the issue with the ICO. Contact details are available on the Information Governance intranet page.

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)
- 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



*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 an IO within their service. The IO must intimate the occurrence of a security incident to the agreed Officer working within the Information Governance Team currently the Team Leader – Information Governance (TL-InfoGov)) Angela Dunlop ext 1944 – dunlopam@angus.gov.uk, who, in the event of a serious breach, will immediately notify the council's Data Protection Officer (the DPO), Anne Garness ext 2003 – GarnessAE@angus.gov.uk . It is important to provide as much information as possible to allow the TL-Info Gov time to review details. There is a requirement to notify the ICO of a breach within 72 hours of the DPO having a reasonable degree of certainty that an incident has occurred. **(See Step 4).**

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

   "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. The **breach checklist** is a useful guide to the facts that need to be established and should be completed by the 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 the TL-Info Gov or in their absence to the informationgovernance@angus.gov.uk (InfoGov mailbox) to ascertain whether the completion of the ICO notification form is required. **(see Appendix 1)**.

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 DPO being aware of referable breaches and therefore, the initial investigation must be concluded and referred to the TL-InfoGov or in their absence, the InfoGov mailbox straight away. , Thereafter the investigation

can be continued as required and further information provided to the TL-InfoGov or InfoGov mailbox when known.

STEP 3 – DPO DETERMINATION

If the TL-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 eg 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 (see Appendix 1), 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 TL-InfoGov or DPO before submission. **(see Appendix 1)**. As a minimum, the following information must be provided:-

- Description of nature of the breach ie 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, reasons for the delay must be provided. Further investigations may result in notification to the ICO that there has not been a breach.

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 breach of GDPR could be a criminal offence. 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 eg 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 eg 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 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

The TL-InfoGov will complete the council's register of breaches. Under the GDPR, 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 and is restricted to viewing by the SIOs, IOs and the DPO.

Details of the entry on the Register will be circulated to all council IOs as a means of sharing lessons learnt and to improve awareness of breaches and best practice.

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

Information Commissioner's Office

Can I report a breach online?

If you have experienced a data breach and need to report it to the ICO but you're confident you have dealt with it appropriately, you may prefer to report it online. You may also want to report a breach online if you are still investigating and will be able to provide more information at a later date. The online form can also be used to report breaches outside our normal opening hours.

Personal data breach reporting form (Right click on the link and select 'Save Link As' or 'Save Target as' to download the form before you begin to edit it.)

If you are reporting online please make sure you include the telephone number of someone familiar with the breach, in case we need to follow up with you about any of the information provided.

If you are unsure about any of the questions within the form, or if have any concerns about how to manage the breach please call us, 0303 123 1113.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

https://ico.org.uk/for-organisations/report-a-breach/#GDPR