Data Protection Act 2018
Personal Data Breaches: reporting requirements, guidance and procedures

Reporting requirements at a glance:

	Information Commission	**Data Subject(s)**
	Personal data breaches likely to result in a **risk** to the rights and freedoms of an individual	Personal data breaches likely to result in a **high risk** to the rights and freedoms of an individual
What is the **timescale** for notification ?	Within 72 hours	Without undue delay
What must we notify ?		
Nature of breach	√	√ In clear and plain language
Types and approx. number of data subjects concerned (e.g. children, elderly people, employees, customers etc)	√	
Types of personal data (e.g. health data, financial details, names and addresses etc)	√	
Approx. number of records concerned	√	
Contact details for the DPO	√	√
Likely consequences of breach	√	√
Measures takes / to be taken to address the breach	√	√
Measures taken / to be taken to mitigate adverse effects	√	√

But please refer to the detailed guidance that follows.

Why is it important to identify and report personal data breaches ?

By law we are required to report some data protection breaches to the Information Commissioner within 72 hours of the beach occurring. In certain circumstances, the breach must also be reported to the individual(s) whose data is involved in the breach. If we fail to report a notifiable breach, or don't do so in a timely manner, it can face a significant fine from the Information Commissioner, as well as being fined for the breach itself.

It is also important that we:

- take action quickly to reduce the impact of data protection breaches on both the affected individuals and the Council; and
- learn from the breach and take steps to prevent a recurrence.

This guidance therefore sets out what we will do in the event of a personal data breach.

What is a personal data breach ?

"Personal data breach" is defined very widely and is not confined to the loss or theft of personal data. Article 4(12) GDPR defines a personal data breach as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

There are 3 broad types of personal data breach:

Confidentiality breach	Unauthorised or accidental disclosure of, or access to, personal data
Availability breach	Accidental or unauthorised loss of access to, or destruction of, personal data
Integrity breach	Unauthorised or accidental alteration of personal data

Examples of personal data breaches:

- attack by malware or ransomware
- access by hacking
- loss of data in the post or in transit
- email or letter sent to wrong person, deliberately or accidentally
- lack of access due to power failure
- loss or mis-use of data by a contractor /
- data unavailable as password lost
- theft of the data
- non-secure disposal of the data
- unauthorised sharing of the data, deliberately or accidentally
- loss of access due to technology failure
- loss or theft of a device containing data
- alteration of data without permission

agent of the Council

But remember – not all personal data breaches need to be reported to the Information Commission, or to the affected individuals (see the reporting requirements below). The Council's Data Protection Officer (or her Deputy etc) will decide whether a breach must be reported to the Information Commission and the affected individuals

"Near misses"

"Near miss" incidents should be reported to the Data Protection Officer. It will probably not be necessary to notify the Information Commission of such incidents, but the Council will be able to learn lessons before a breach occurs – we can take action to strengthen our policies and procedures and can arrange any appropriate staff training.

What are the notification requirements ?

The notification process is summarised the flowchart in Appendix 1

Informing the Information Commission

Article 33(1) GDPR says that we must notify the Information Commission of a personal data breach "without undue delay, and where feasible, not later than 72 hours after having become aware of it ……. unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" and, where the Information Commission is not notified within 72 hours, the notification "shall be accompanied by reasons for the delay".

Notification should take place within **72 hours** of the Council becoming aware of the data breach if the Data Protection Officer concludes that the breach presents a risk to the rights and freedoms of the affected individuals.

The Council may not be able to comply fully with the notification requirements within this timescale as not all the required information may be available. However, the Information Commission will accept notification in phases provided the Council works to provide all the information in a timely manner. At this first notification stage we should also seek advice about whether it is necessary to notify affected individuals.

We will be deemed to have "become aware" of a personal data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This will depend on the circumstances – sometimes it will be obvious that there has been a breach but sometimes it may take time to establish if personal data has been compromised. However, if we are alerted to a possible security incident we will be expected to take prompt action to investigate it to determine whether there has been a personal data breach.

If the Council fails to inform the Information Commission about a notifiable breach we could face a fine of up to £8.9 million.

Informing affected individuals

Article 34(1) GDPR says that we must notify affected individuals without undue delay where a personal data breach is likely to result in a **high risk** to their rights and freedoms. The main aim of this is to enable people to be provided with specific information about the steps they can take to protect themselves from any negative consequences of the breach.

For example, a personal data breach could lead to a high risk of discrimination, identity theft or fraud, financial loss, emotional distress or damage to reputation. Where the personal data reveals a person's racial or ethnic origin, political opinion, religion, trade union membership, health information or information about their sex life or criminal convictions then a risk should be considered to exist.

When assessing risk you should the possible impact on the individual and the likelihood of an adverse impact occurring. When doing this you should consider the following:

- the type of breach (e.g data being destroyed may have less risk than an unauthorised disclosure)
- the nature, sensitivity and volume of personal data (e.g. a combination of personal data is usually more sensitive than a single piece of personal data)
- the ease of identification of individuals
- the severity of consequences for individuals (e.g. vulnerable people could be at greater risk, the risks are higher where the data could be used for identity theft)
- any special characteristics of the individual (e.g. a breach may have a greater effect on children or vulnerable adults)
- the number of affected individuals

If the impact on an individual has the potential to be severe then it is likely that there will be a high risk to their rights and freedoms.

If we need to contact affected individuals we should do so directly unless this involves a disproportionate effort. There may be a disproportionate effort if a significant number of individuals are involved or if, as a result of the breach, the individual's contact details have been lost. In such circumstances we are required to communicate the breach publicly in an effective and transparent manner – this could include a prominent website banner or a prominent press advert. A press release on its own would not be sufficient.

Even if the Council doesn't consider notification to be necessary, the Information Commission can require us to notify affected individuals.

Procedure in the event of a data protection breach taking place

1. Staff must notify the Data Protection Officer as soon as possible upon becoming aware of a potential personal data breach. In the absence of the DPO, staff must notify the Deputy Data Protection Officer:

Data Protection Officer	the Executive Director (Legal & Democratic Services	Jane Ellis Ext 2146
Deputy Data Protection Officer	the Head of Audit	Mark Beard Ext2634

   In the absence of either of them, staff must notify either the Chief Executive or the Deputy Chief Executive. It is important that the DPO (or her Deputy etc) is notified of potential breaches as soon as possible, as the Council may need to report the breach to the Information Commission within 72 hours of becoming aware of it.

2. Staff discovering a potential personal data breach must also notify their service manager as soon as possible.
3. Upon being notified of a potential personal data breach the DPO (or her Deputy etc) will:
    a. lead the investigation into the potential breach
    b. take prompt action to determine whether a breach has occurred and, if it has, how the breach happened and what data is affected
    c. if necessary, convene a response team to assist with the investigation including, for example: the relevant service manager, IT, internal audit and legal services
    d. ensure a written record is kept of the investigation and that the breach reporting form is completed
    e. liaise with the Council's press officer in respect of the breach and the proposed response to any media enquiries
    f. determine whether the Police need to be notified of the breach
    g. consider and initiate steps to contain the breach and prevent further breaches
4. As soon as possible, and where feasible, within 72 hours of the Council becoming aware of the breach, the DPO (or her Deputy etc) will assess the severity of the personal data breach and the level of risk it presents to individuals. The DPO (or her Deputy etc) will then determine whether to notify the Information Commission of the breach and reach a preliminary conclusion about whether the affected individuals should be notified and how.
5. The DPO (or her Deputy etc) will notify the Information Commission of notifiable breaches:

Information Commission Breach reporting line	0303 123 1113	Monday to Friday 9.00am to 5.00pm

6. The DPO (or her Deputy etc) will seek the ICO's guidance about whether affected individuals should be notified of the breach and how. If notification is appropriate or required, the DPO will ensure that notification occurs in an appropriate manner.

7. The DPO will complete her investigation into the breach and determine what remedial action is required to reduce the risk of future breaches. The DPO will make any necessary changes to policy and procedure and ensure that appropriate staff training takes place if appropriate.

Record keeping requirements

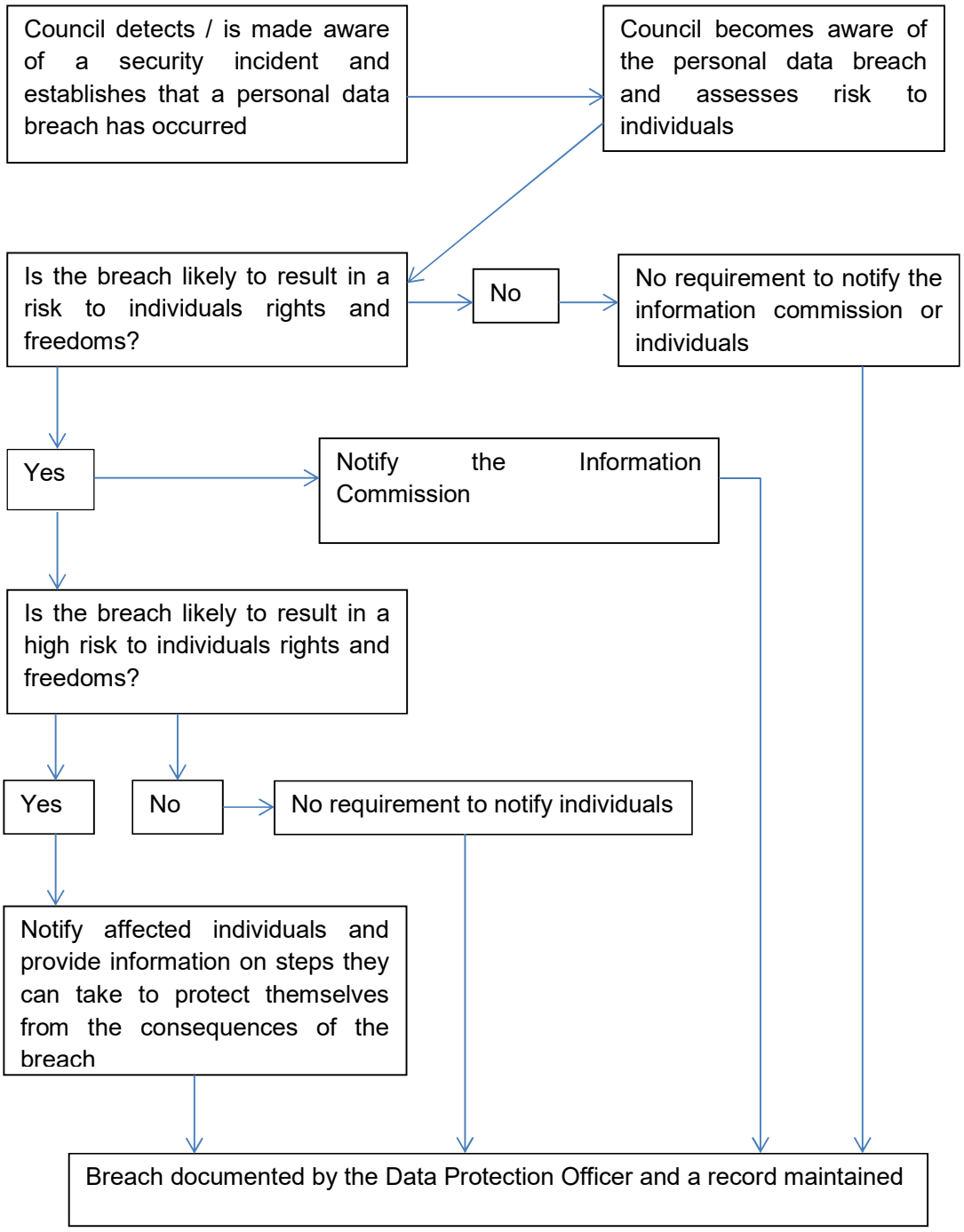
Article 33 GDPR requires certain records to be kept by the Council in respect of all personal data breaches, including those that are not notified to the Information Commission. In particular, this record must include the following:

- cause of the breach
- details of what happened
- details of the personal data affected
- effects of the breach
- remedial action taken by the Council

The Data Protection Officer (the Executive Director (Legal & Democratic Services)) will keep a register of all personal data breaches and all such breaches must be reported to the DPO as soon as staff become aware of them.

The record of each personal data breach will be kept by the Data Protection Officer on a breach reporting form in the format attached to this guidance at Appendix 2.

Appendix 1


Council detects / is made aware of a security incident and establishes that a personal data breach has occurred
Council becomes aware of the personal data breach and assesses risk to individuals
Is the breach likely to result in a risk to individuals rights and freedoms?
No
No requirement to notify the information commission or individuals
Yes
Notify the Information Commission
Is the breach likely to result in a high risk to individuals rights and freedoms?
Yes
No
No requirement to notify individuals
Notify affected individuals and provide information on steps they can take to protect themselves from the consequences of the breach
Breach documented by the Data Protection Officer and a record maintained

Appendix 2

Data Protection – breach reporting form

This document will form the Council's record of any data protection breach.

It will be completed by the Data Protection Officer who will retain a copy for future reference.

It may not be possible to complete all of the form immediately after a data breach is discovered, but the form will be updated as the investigation into the breach progresses.

REPORTING:	
Date and time data breach discovered	
Service Area	
Date and time breach reported to the DPO	
Name of reporting officer	
Breach reported to the Information Commission ?	YES / NO
Date and time breach reported to Information Commission	
If the breach was not reported to the Information Commission, explain why	
Breach reported to individual(s) affected ?	YES / NO
Details of how and when affected individuals were notified	

DETAILS OF BREACH:	
Date and time the breach occurred	
Nature of breach (e.g unauthorised disclosure, hacking, theft etc)	
Did the breach involve a Council contractor or partner organisation ? Please give details	
Description of how breach occurred	
How did we become aware of the breach ?	

DETAILS OF PERSONAL DATA:	
Description of data involved	
Approx. number of individuals affected	

IMPACT OF BREACH:	
Is there anything to suggest that the personal data has been mis-used ?	
Describe the risk of harm to individuals as a result of the breach	
Has the Council received any complaints as a result of the breach ?	
Has there been any media coverage in respect of the breach ?	

RESPONSE TO BREACH:	
Has the data been retrieved or deleted ? Please give details of when and how	
What remedial action has been taken ?	

LESSONS LEARNED:	
What action has been taken to minimise the risk of a similar breach occurring in the future ?	