Reporting Personal Data Breaches

Policy and Procedures

August 2019

Contents

1 Introduction

The Personal Data Breaches Policy and Procedures sets out Fenland District Council's approach to personal data breaches and the procedure to take in the event of one.

Personal data breaches are a high risk for the council due to the volume of personal data held and processed in everyday activities. The General Data Protection Regulations 2018 (GDPR) and the Data Protection Act 2018 (DPA) have introduced a higher monetary fine for severe data breaches with a cap of 20 million Euros. Alongside this, severe data breaches can also have a detrimental effect on the council's reputation.

Fenland District Council is committed to reducing the chances of data breaches across the council and dealing with these in line with the Information Commissioners Office's (ICO's) requirements as outlined below.

2 Definitions

"Personal data" means any information relating to an identified or identifiable individual ('data subject'); an identifiable individual is someone who can be identified, either 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 individual.

The definition of a "personal data breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach includes, but is not restricted to, the following:

- The accidental alteration or deletion of personal data
- The transfer of personal data to those who are not entitled to receive it
- Unauthorised access to personal data
- Use of personal data for purposes for which it has not been collected and which go beyond those uses that the data subject could reasonably have contemplated
- Theft of storage devices

3 Policy Statement

Fenland District Council will seek to avoid personal data breaches. The council recognise a personal data breach, if not addressed in an appropriate and timely manner, can result in physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data

protected by professional secrecy, or any other significant economic or social disadvantage to the individual concerned. Where personal data breaches do occur the council will, without undue delay, seek to contain the harm to individuals, investigate the breach, report the breach to the Information Commissioner's Office and look to learn the lessons from any actual or suspected breaches.

4 Scope

This document applies when a personal data breach is suspected. The policy and procedure it sets out is to be followed by all Councillors, officers, contractors and agents of the council who use council facilities and equipment, or have access to, or custody of, personal data collected by the council.

5 Aims and Objectives

The aim of this policy and procedure is to ensure that the council reacts appropriately to any actual or suspected personal data breaches in accordance with GDPR.

6 Relevant reference documents

This policy has been written in reference to various legislations, most notably:

- The Data Protection Act 2018
- The General Data Regulation 2018

This document should also be read in unison with the council's other data protection policies, most notably the:

- Data Protection Policy
- Information Management Policy
- Information Security Policy

7 Roles and Responsibilities

All employees are responsible for reporting any data breaches to the Data Protection Officer. The Data Protection Officer for Fenland District Council is Anna Goodall who can be contacted at agoodall@fenland.gov.uk.

The Data Protection Officer is responsible for dealing with any breaches within the council as and when they occur. She must inform individuals of breaches to their data if required and report any serious breaches to the ICO.

8 Risks

The council recognises that there are risks associated with the collection, use transmission and storage of personal data in order to conduct official council business. By following this policy and procedure, suspected data breaches should be identified quickly and the impact of personal data breaches should be reduced. This policy shall ensure that suspected personal data breaches are followed up correctly and shall help identify areas for improvement.

Non-compliance with this policy and procedure could result in significant detrimental effects on individuals and the council being heavily fined and/or its reputation being damaged. Individuals can also be liable in certain cases and can be personally fined and suspended under data protection legislation.

9 Procedure for reporting personal data breaches

Appendix 1 provides a high level process flow diagram illustrating the process to be followed when reporting suspected or actual personal data breaches.

Personal data breaches need to be reported to the councils' Data Protection Officer at the earliest possible stage as the council has a duty to report any personal data breach to the Information Commissioner's Office (ICO) within 72 hours unless the ICO has issued guidance to the contrary.

The information provided to the Data Protection Officer should include as much detail as possible of the personal data breach, those affected and the consequences. A form is available on the Intranet to report a personal data breach – if not completed at the time of the actual report, it must be completed immediately afterwards. The Data Protection Officer and Member Services can assist in completing the form. The reporting of a suspected personal data breach should not be delayed however while the information is being gathered. The Data Protection Officer will make an assessment of whether the personal data breach passes the threshold (if any) set by the ICO for personal data breaches to be reported to the ICO. The Data Protection Officer will also make an assessment of the risk to the data subject. If the Data Protection Officer concludes that the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, for example, where there is a risk of identity theft, she will notify the data subject directly.

The Data Protection Officer will notify the Senior Information Risk Owner (SIRO) who is Carol Pilson for the council, the Chief Executive and the Corporate Management Team (CMT) as soon as possible after receiving a report of a personal data breach. The SIRO, Chief Executive, Data Protection Officer, and CMT will agree what measures should be taken to deal with the personal data breach.

When reporting the breach to the ICO the Data Protection Officer will include the following information:

- The nature of the personal data breach including, where possible
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the data protection officer or other contact point where more information can be obtained

- A description of the likely consequences of the personal data breach

- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects

In the event that it is not possible to report the personal data breach to the ICO within 72 hours, the notification will also give the reasons for the failure to do so.

10 Policy Compliance

If any officer is found to have breached this policy and procedure, they may be subject to the council's disciplinary procedure. If any Councillor is likewise found to have breached the policy and procedure a complaint will be made to the Conduct Committee. In either case if a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Data Protection Officer or SIRO.

11 Policy Governance

The following table identifies who within the council is Accountable, Responsible, Informed or Consulted with regards to this policy and procedure. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.

- Accountable – the person who has ultimate accountability and authority for the policy.

- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.

- Informed – the person(s) or groups to be informed after policy implementation or amendment.

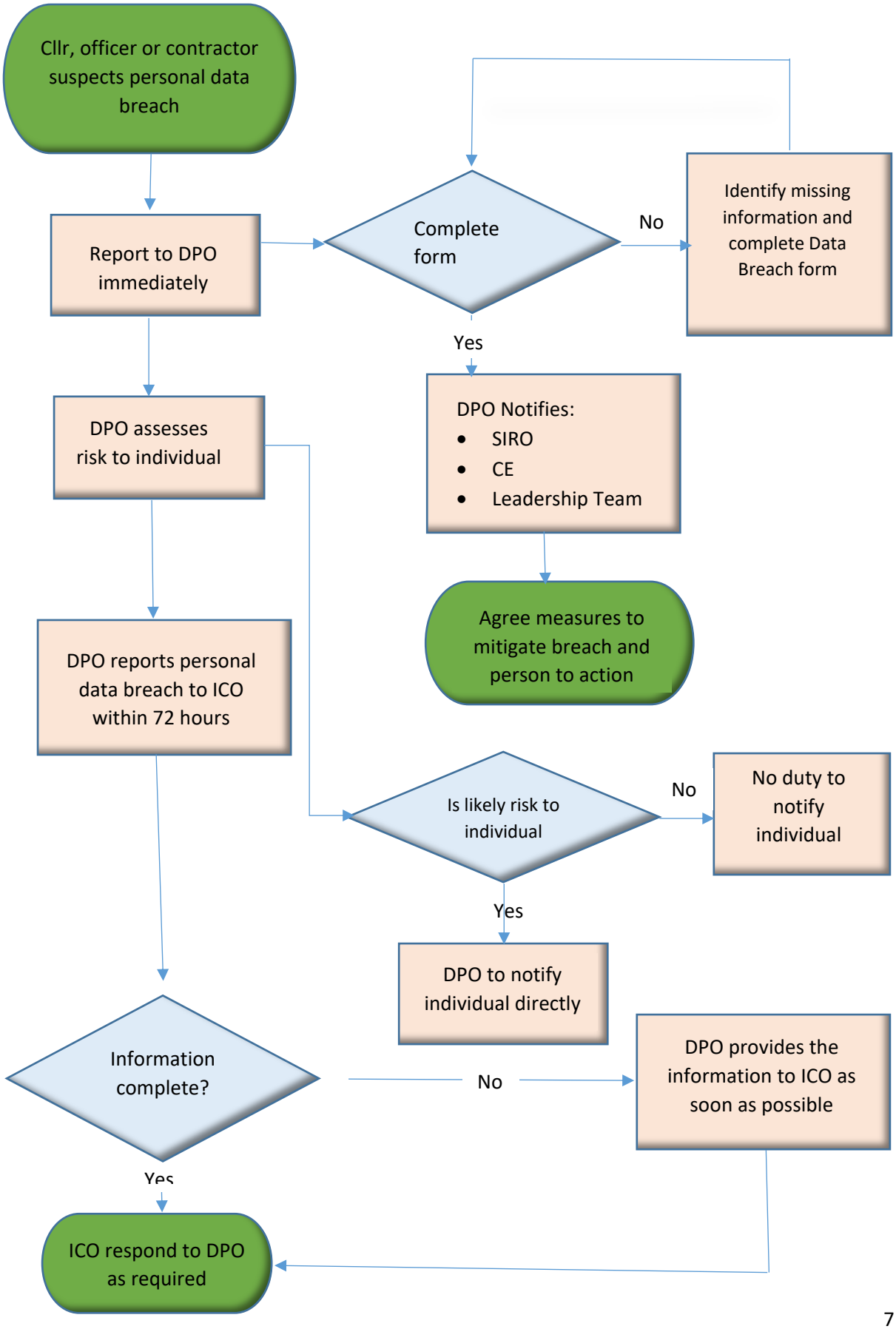
Responsible	Data Protection Officer
Accountable	Chief Executive
Consulted	Senior Information Risk Owner, Management Team
Informed	All Councillors, officers, contractors and agents.

12 Key Messages:

- A personal data breach is more than just losing personal data

- Personal data breaches can have significant impacts on individuals
- The council has a duty to notify the ICO of any personal data breach and may have to inform individuals directly
- All Councillors, officers, contractors and agents of the council should report any suspected personal data breaches immediately
- There are potentially heavy fines for failing to report personal data breaches to the ICO

Appendix 1 – Process Flow; Reporting a personal data breach



Appendix 2 - Breach Matrix – Including Impact Criteria

Breach Types
Lost in Transit - The loss of data (usually in paper format but may also include CDs, tapes, DVDs or portable media) whilst in transit from one service area to another. May include data that is: • Lost by a courier • Lost in the 'general post' (i.e. does not arrive at its intended destination) Lost whilst on site but in situ between two spate buildings or services (I.e. Housing to Accountancy)
Lost or stolen hardware - The loss of data contained on fixed or portable hardware. May include: • Lost or stolen Laptops • Hard drives • Pen drives • Servers • Cameras • Mobile phones – containing personal data • Desk-tops / other fixed electronic equipment • Imaging equipment containing personal data • Tablets The loss or theft could take place on or off a data controllers premises. For example the theft of a laptop from an employee's home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk
Lost or stolen paperwork - The loss of data held in paper format would include any paper work lost or stolen which could be classified as personal data examples would include: • Housing assistance forms • Letters • Complaints • Registers • Officers notebooks The loss or theft could take place on or off a data controllers premises. For example the theft of paper work from an employee's home or car, or a loss of a portable device whilst travelling on public transport.
Disclosed in Error - This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This could include situations where the information hasn't actually been accessed. Examples include: • Letters / assessments / files been sent to the wrong individuals • Verbal disclosures made in error • Failure to redact personal information from documentation to the requester or third parties – particularly in regards to DSARs • Inclusion of information relating to other data subjects in error – again particularly DSARs • Emails / faxes sent to the incorrect individual or with the incorrect information attached • Failure to blind carbon copy emails Mail merge / batching errors on mass mailing campaigns leading to the incorrect

individuals receiving personal data
Uploaded to website in error - This category is distinct from disclosure in error as it relates to information added to a website containing personal data which is not suitable for disclosure. It may include: • Failures to carryout appropriate redaction • Uploading the incorrect documentation
Non-secure disposal of hardware - The failure to dispose of hardware containing personal data using appropriate technical and organisational means. It may include: • Failure to meet principle 6 of GDPR (Security) when employing a third party processor to carry out the removal / destruction of data • Failure to securely wipe data prior to destruction • Failure to securely destroy hardware to appropriate industry standards Re-sale of equipment with personal data still intact / retrievable
Non-secure disposal of paper work - The failure to dispose of paper work containing personal data using appropriate technical and organisational means. It may include: • Failure to meet principle 6 of GDPR (Security) when employing a third party processor to remove / destroy / recycle paper • Failure to use confidential waste destruction facilities Data sent to landfill / recycling intact
Technical security failure (including hacking) - The category concentrates on the technical measures a data controller should take to prevent unauthorised processing and loss of data and would include: • Failure to secure systems from inappropriate / malicious access • Failure to build website / access portals to appropriate technical standards • Failure to protect internal files sources from accidental / unwarranted access (for example failure to secure shared file spaces) In respect of successful hacking attempts, the ICO's interest is in whether there were adequate technical security controls in place to mitigate the risk
Corruption or inability to recover electronic data - Avoidable or foreseeable corruption of data or an issue which otherwise prevents access which has quantifiable consequences for the affected data subjects e.g. disruption care / adverse clinical outcomes, for example: • The corruption of a file which renders the data inaccessible The inability to recover a file as its method / format of storage is obsolete
Unauthorised access / disclosure - Wilful unauthorised access to, or disclosure of, personal data without the consent of the data controller
Other - This category is designed to capture the small number of occasions on which breach occurs which does not fall into the aforementioned categories. These may include: • The sale or recycling of office equipment (for example filing cabinets which later are found to contain personal data) Inadequate controls around physical employee access to data leading to the insecure storage of files (for example failure to implement a clear desk policy or insufficient lockable filing cabinets and storage)

Appendix 3- Data breach reporting form

Form GDPR 1 – Reporting personal data breaches	
Name of person making the report	
Contact details	
The nature of the personal data breach e.g. alteration or deletion of personal data, transfer to third party not entitled to it etc.	
When did this occur (Date)?	
How did the personal data breach occur?	
Which individuals are affected by the personal data breach (include categories and approximate number of individuals concerned)?	
How many personal data records are concerned?	
How are the individuals likely to be affected by the personal data breach?	
Have any measures been taken or proposed to be taken to deal with the personal data breach? List in next column	
Have any measures been taken or proposed to be taken to mitigate any possible adverse effects? List in next column	

Signed by the person reporting the personal data breach, date and time	

To be completed by the Data Protection Officer

Received by Data Protection Officer date and time	
Is the information complete?	Yes / No If No, what further information is required?
Details of personal data breach reported to: a) ICO b) Chief Executive c) Leadership Team	Yes / No – When: Yes / No – When: Yes / No – When:
What measures have been agreed/ should be taken to deal with the personal data breach?	
What measures have been agreed / should be taken to mitigate harm caused by the personal data breach?	
Personal data breach reported to the ICO?	Yes / No – When:
Is the personal data breach likely to result in a high risk to the rights and freedoms of the individuals concerned? If Yes individuals must be notified	Yes / No – When:

directly	

Impact Criteria

Impact Levels	Harm Criteria	Damage to council's reputation with the possibility of regulatory action and subsequent legal action from the data subjects against the council or council employees	Data Subject		
			Confidentiality	Integrity	Availability
1	*Negligible*	Minor harm to an individual, individuals or small group which could result in some publicity in the local media. No legal or regulatory consequences	Public information disclosed	Public information corrupted	Public information lost
2	*Low*	Harm to an individual, individuals or small group which could result in publicity in the local media and social media. Some legal or regulatory notification might be needed (i.e. advice from the ICO might be sought)	Semi Public or minor identifying information disclosed	Semi Public or minor identifying information corrupted	Semi Public or minor identifying information lost
3	*Moderate*	Minor damage or distress to an individual, individuals or a group, which could result in adverse publicity in traditional national media. Some legal or regulatory sanction (Notifiable)	Identifying information disclosed	Identifying information corrupted	Identifying information lost
4	*High*	Damage and distress to an individual or substantial number of individuals which could result in sustained adverse publicity in national and social media. Significant legal or regulatory sanction (Notifiable)	Identifying information disclosed	Identifying information corrupted	Identifying information lost
5	*Very High*	Significant damage and distress to an individual or high number of individuals which could result in sustained adverse publicity across all media platforms.	Sensitive information disclosed	Sensitive information corrupted	Identifying information lost

		Major legal or regulatory sanction (Notifiable)			

Version control

Policy name	Reporting Personal Data			
Policy description	Outline of Fenland District Council's approach to data breaches and how we shall deal with them.			
Responsible Officer	Data Protection Officer/IT Manager			
Version number	Date formally approved	Reason for update	Author	Review date
V01	August 2019	Creation of data breach policy and procedure	Data Protection Officer/IT Manager	August 2020
V1.1	February 2020	Alteration of structure to fit FDC policy template, inclusion of version control table and contents table.	Data Protection Officer/IT Manager	February 2021