DATA INCIDENT AND BREACH MANAGEMENT PROCEDURE

Version 2
Date 1st February 2021

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available only at the Published Location stated in the Document Control Section.

Version Control

Version	Date Created	Author	Update Information
V1.00	10th May 2018	Gerry Mahon	
V2.00	1st February 2021	Rose Johnston	Updated to reflect current legislation and guidance

Document Control

Title	Corporate Guidance on reporting and management of data incidents & breaches
Intended Audience	Employees and elected members who handle personal and sensitive personal (special category) information about individuals
Prepared By	Rose Johnston Information Governance Officer
Published Location	Intranet
Other documents referenced	Data Protection Policy
	Reporting Security Incidents

Contents

1 Introduction

East Renfrewshire Council as a data controller has a legal responsibility to ensure that personally identifiable information about living individuals is processed securely, held confidentially and with integrity and accessed only by those who have a justified right of access.

The Council has a duty to ensure that all personal information is processed in compliance with the principles set out in the Data Protection Act 2018 (DPA2018)

Principle 1	Personal data shall be processed lawfully, fairly and in a transparent manner
Principle 2	Personal data shall be collected for specified, explicit and legitimate purposes
Principle 3	Personal data shall be adequate, relevant and not excessive.
Principle 4	Personal data shall be accurate and, where necessary, kept up to date
Principle 5	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed
Principle 6	Personal data shall be processed in a manner that ensures appropriate security of the personal data

It is expected and is the responsibility of each Service to ensure that there is compliance with DPA2018 and that suitable processes and procedures are in place for employees to follow when handling or managing personal information assets.

These procedures provide advice and guidance on the management of data incidents that ensures the Council complies with data protection legislation.

It is vital that the details of an incident are established quickly as it may be necessary for the Council's Data Protection Officer (DPO) to report an incident to the UK Information Commissioner (ICO). The DPO must action this within 72 hours of becoming aware of an incident.

Failing to report an incident or doing so late may result in sanctions or penalties being levied against the Council.

This document sets out the steps to take that should something go wrong and an incident occurs, the employee knows what action to take:

- to ensure the correct reporting mechanisms are followed; and the
- Council is compliant with its obligations under the DPA2018

It is important that all our employees understand what a data incident or breach is and are aware of the relevant steps (see figure 1) within the data incident and breach response lifecycle.

Figure 1 - Data Incident & Breach Response Life-Cycle

2 Scope

They apply to all Employees and Elected Members of the Council, both permanent and temporary. Where non-council organisations or those that we work in partnership have access to our information assets these procedures equally apply.

These procedures apply to any suspected data incident in relation to both paper and electronic records containing personal data held by the Council or held by a data Processor on the Council's behalf.

3 What is a data incident?

A **breach of data protection** is an incident in which sensitive, confidential or otherwise protected personal data has been accessed and/or disclosed in an unauthorised manner.

A **security breach** is an incident that results in unauthorised access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.

A **security breach** may also be a **data breach** if personal data is copied, transmitted, viewed, stolen or used by an individual who is not authorised to do so or who has no right of access or justifiable purpose in accessing the data and leads to an increased risk of harm of any kind to an individual or individuals.

A data breach can happen for many reasons:

- Loss or theft of data or equipment (encrypted and non-encrypted devices) on which personal is stored
- Inappropriate access controls allowing unauthorised use or access to personal data
- Human error
- Insecure disposal of paperwork containing personal data
- Loss of or theft of paper record files containing Council data
- Unforeseen circumstances such as fire or flood
- Equipment failure
- Erroneously sent emails, correspondence

- “Blagging” offences where information is obtained by deceit
- Deliberate acts carried out by individuals from inside the controller or processor’s organisation
- Cyber-attacks (hacking, malware ransomware, phishing)
- Alteration of personal data without permission
- Loss of availability of personal data

4 Responsibilities under these procedures

4.1 All employees and elected members are expected to familiarise themselves with the definition of a data incident, to recognise such incidents as and when they occur and to report them within the appropriate timescales to the DPO. Employees may also be asked to assist in the investigation of a data incident.

4.2 The Service will coordinate the investigation of suspected breaches relating to records within their own departments and will provide the DPO with all necessary information and assistance to allow the DPO to intimate the breach to the Information Commissioner’s Officer (ICO).

4.3 The DPO will report any suspected breach to the Information Commissioner’s Office (ICO) on behalf of the Council and act as the council’s link to the ICO as regards the progress of any subsequent investigation.

5 Reporting Process

All employees are expected to remain vigilant and ensure that the Council’s use of personal data complies with the 6 data protection principles and the Data Protection Policy. However where this does not happen it is vital that incidents are reported in accordance with the procedures defined within this document.

5.1 The details of an incident must be established quickly for an assessment to be undertaken and for an initial evaluation to be made within **24 hours.**

5.2 This may include an initial response to investigate and contain the situation but may also be necessary to create a recovery plan implementing damage limitation where necessary.

5.3 Where a security breach as defined within the Reporting Incidents section of is identified you must follow that process. Where it is identified that personal data has been lost or compromised the Information Security and Digital Risk Officer will inform the DPO.

6 Notification

A report should be emailed by to the DPO using the form exampled in Appendix 1, **within 3 hours** from the discovery of or suspected incident coming to light irrespective of whether the investigation has concluded or all information has been obtained.

It is vital that full, open and honest answers are provided as failure to do so could lead to additional regulatory sanctions.

7 Initial Assessment

7.1 An assessment should be undertaken to verify the potential impact on those affected by the incident and ensure containment and recovery action is promptly undertaken.

Steps may include:

- Advising actions taken to mitigate any potential harm or ensure any information leakage is ceased or recovered including;
    - Detailing any organisational or technical measures which can be undertaken to minimise impact of breach.
- Confirming the current safeguards in place to protect personal data including;
    - details of local operating processes;
    - advising data protection and information security training undertaken by employees;
    - informing the steps being taken or considered to strengthen safeguards to prevent a re-occurrence.

7.2 The Service upon receipt of the report will liaise with the DPO and will forward a copy of the incident report by email to the DPO at dpo@eastrenfrewhire.gov.uk.

7.3 On notification the DPO will undertake an assessment of the incident based on the information presented and liaise with nominated Service representative. This task may be delegated to suitable employees of their choosing who will be advised of any particular issues that require specific attention.

At this stage the incident investigation need not have concluded and the data breach need not have been confirmed.

7.4 The DPO may instruct the Service to implement measures identified in Section 5

7.5 Where it is identified there is a technical failing in relation to Council systems the DPO should liaise with the Information Security and Digital Risk Officer to identify any steps available to minimise the impact of the breach.

8 Containment & Recovery

8.1 Containment and recovery is a crucial step in mitigating risk arising from a data incident or potential breach and the service must cooperate with the

DPO to ensure that appropriate and effective steps are taken to minimise the impact.

8.2 This includes identifying a named officer to be available to work with the DPO and ensuring swift action is taken to rectify the underlying issue that has resulted in the incident.

8.3 Once the initial incident is contained, the DPO will undertake a review of the causes leading to the incident.

8.4 Where the DPO considers or is instructed by the data controller, that a formal investigation be carried out, a report on the matter will be prepared and issued to the relevant Information Asset Owner, Senior Manager and/or the relevant Head of Service.

9 Assessment of Risk by DPO

9.1 Based on the information available the DPO will assess the likelihood and severity of the risk to data subject rights caused by the incident. In consideration with regard to the nature and extent of any impact resulting from the incident the DPO will consider the following;

- The nature of the information involved (in particular whether it includes special category or criminal conviction data)
- The volume of information and the likelihood that the incident could cause distress, financial or physical harm or any other detriment to the data subject.
- Factors which reduce the risk to the data subject. For example encryption of lost information, known trusted recipient of accidental disclosure, or satisfaction that there is no further disclosure.

9.2 Should the DPO determine that the incident is likely to result in a risk to individuals' rights and freedoms they will notify the Information ICO within 72 hours after the incident first comes to light. This is irrespective of whether the investigation has concluded or all necessary information has been obtained.

9.3 If a decision is taken to notify individuals of the breach or the ICO instructs the Council to notify, such notification will also inform individual/s how and when the breach occurred and what data was involved.

9.4 It may be necessary for the DPO to inform individual/s what has happened where there has been a serious incident, and also what we are doing to respond to the breach and to advise of any remedial measures to take to minimise the impact upon them. It may also be necessary in certain cases to inform other organisations (such as Police Scotland or NHS).

9.5 The DPO shall obtain contact details for affected individuals from the relevant Service DPO.

9.6 The DPO should consider whether a report requires to be made to the Police if the incident suggests that a crime has been committed.

10 Reporting & Recording Breaches

10.1 Based upon the nature and seriousness of the breach and the adequacy of any remedial action a formal report will be prepared and issued by the DPO.

10.2 This will contain a lessons learned and a risk assessment section and any identified actions will be documented for the Service to take forward.

10.3 Regardless of whether the incident/breach requires to be reported to the ICO the DPO will record it as part of the Council's Log of Incidents and will record the facts of the incident, its effect and remedial action taken to address it.

10.4 The DPO will also record the cause and recommend steps to prevent a reoccurrence. Such steps may include staff training, improving or new procedures or changes in technology.

11 ICO Outcomes

11.1 Where there has been an ICO involvement and the Council is instructed to undertake remedial action this will be communicated to the relevant Information Asset Owner.

11.2 Where it is communicated by the ICO that formal enforcement action will be taken the Chief Executive and the relevant Director will be informed by the DPO.

12 Discipline

12.1 If a data incident occurs as a result of the failure of an employee to follow appropriate processes or procedures in relation to the handling pf personal data, they may be subject to disciplinary action in terms of Section 5 – Reporting Process

12.2 Where an employee knowingly fails to report the existence of a possible data incident/breach that failure shall constitute gross misconduct under the Council's Disciplinary Policy and may give rise to disciplinary action against the employee concerned.

For further advice or assistance with data protection please contact the Information Governance Officer in the first instance either by email or by telephoning 0141 577 3344.

Appendix 1 - Data Incident Reporting Form

Data Incident Reporting Form		
Directorate & Service Area		
Service Contact Name		
Contact Details		
Notification		
Date & Time of Incident (if not known when is it believed to have occurred/ when was it discovered?)		
If system breach – name of system		
Is it a failure to comply with local operating procedures/processes?		
Initial assessment		
How was incident reported to the Council or discovered?		
List the data identifiers exposed e.g. name, dob, health information	**Personal Data**	
	Special Category Data	
	Criminal Conviction Data	
Describe how the incident occurred		
Number of records affected		
How many data subjects (individuals) are involved or could be affected?		
Categories of Data Subjects (e.g. employees, pupils, vulnerable children/adults		
Detail the safeguards and security measures in place to help ensure personal data is managed in accordance with the data protection principles? For example local operating procedures/ guidance/training		
Containment & Recovery		
Describe actions being taken to mitigate any ongoing potential harm or ensure any information leakage is contained i.e. describe the protective measures taken		
Is there an ongoing risk of harm to those involved or impacted by the incident?	**Yes /No (delete as appropriate)**	
If yes, describe what the likely harm may be		
Are the individuals aware of the incident?		

If yes, detail how they became aware of the incident e.g. they notified you/learned about it from another party/social media	
Have you received a formal complaint from individuals involved?	**Yes /No (delete as appropriate)**
If yes, provide details and attached any correspondence received and issued along with completed report to DPO.	
Are other organisations involved in the incident?	**Yes /No (delete as appropriate)**
If yes, provide details including contact information and provide details of any discussions with them	
What steps are being taken or considered to strengthen safeguards to prevent a re-occurrence?	
Training	
Have all employees involved in incident (where identities known) undertaken training in data protection and information security within the last 2 years?	**Yes /No (delete as appropriate)**
If Yes, confirm data and type of training undertaken in the last 2 years	
If No, does the Service intend that they undertake refresher training?	
Is it intended service operational guidance and/or local procedures be updated? If yes provide details and expected completion timescales	
Additional Information	
Senior Manager/HOS notified	**Yes/No (delete as appropriate)**
Name of Senior Manager/HOS	
Data report emailed to DPO	