Eden District Council

Town Hall, Penrith, Cumbria CA11 7QF
Tel: 01768 817817
Email: info.governance@eden.gov.uk

Approved by: Executive
Date Approved: 4 December 2018
Review Date: April 2020
Responsible Officer: Deputy Chief Executive

Personal Data Breach Policy

Accessibility Information

A summary of the information contained in this document is available in different languages or formats upon request. Contact Eden District Council's Communication Officer, telephone: 01768 817817 or email: communication@eden.gov.uk

Document Control

Document Control	
Organisation	Eden District Council
Title	Personal Data Breach Policy
Author	Information Governance Manager
Filename	PersonalDataBreachPolicy_v1.0.doc
Owner	Deputy Chief Executive
Subject	Data Protection and Information Security
Protective marking	UNCLASSIFIED
Review date	April 2020

Document Amendment History			
Revision No	**Revised by**	**Date of Change**	**Description of Change**
0.1	Information Governance Manager	June 2018	First draft
0.2	Information Governance Manager	November 2018	Minor amendments
1.0	Information Governance Manager	14 November 2018	Final version

Approval	**Date**
Chief Finance Officer and Monitoring Officer governance checks	14 November 2018
Executive	4 December 2018

Contents

1. Statement

1.1 We are committed to protecting individuals' personal data and privacy and will seek to have in place robust breach management processes, to comply with the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and other privacy laws.

1.2 We will seek to use appropriate technical and organisational measures to protect the information and personal data we process. However, whatever safeguards are in place, the potential for a personal data breach will always exist. Therefore, we will manage any incidents that may arise, quickly and effectively and in compliance with the law, to minimise the level of risk to people's rights and freedoms.

2. Purpose

2.1 The purpose of this policy is to set out the procedure for the Council's approach to managing personal data breaches. It explains how we will meet our duties for breach detection, notification, containment and recovery, assessing risk, investigation, recording, evaluation and implementing controls for the prevention of any future recurrences.

2.2 It is important to have in place a standardised approach across the Council in the event of a personal data breach. To ensure a standardised approach, this policy is supported by a Personal Data Breach Response Protocol and Internal Data Breach Notification Form which are internal documents, available to all authorised users, setting out in greater detail the practical steps for managing a breach.

3. Scope

3.1 This policy applies to all authorised users of the Council's information systems, including employees, Elected Members, contractors, agents and partners who process personal data on behalf of the Council.

3.2 This policy applies to all personal data processed by or on behalf of the Council relating to an identified or identifiable living individual and held on all types of media, throughout the lifecycle of the information, from its receipt or creation, storage and use, to disposal.

4. Definitions

4.1 A personal data breach is defined under GDPR 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.' It can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. This can include breaches that result from both accidental and deliberate causes.

4.2 Not all personal data breaches involve the loss or theft of personal data. A breach could involve access by an unauthorised party, alteration of data without permission, sending personal data to an incorrect recipient, or loss of availability due to an IT system outage. The different types of personal data breach can be categorised according to the three information security principles:

- Confidentiality breach - an unauthorised or accidental disclosure of, or access to personal data;

- Integrity breach - an unauthorised or accidental alteration of personal data;
- Availability breach - an unauthorised or accidental loss of access to, or destruction, of personal data.

5. Legal and Regulatory Requirements

5.1 We will seek to comply with all relevant legislative and regulatory requirements in relation to personal data breaches.

5.2 GDPR makes it compulsory for organisations to report a personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware, if it likely to result in a risk to people's rights and freedoms. We will seek to comply fully with these requirements, including the following provisions under GDPR:

- Article 28 - Processor;
- Article 32 - Security of processing;
- Article 33 - Notification of a personal data breach to the supervisory authority; and
- Article 34 - Communication of a personal data breach to the data subject.

6. Roles and Responsibilities

6.1 All authorised users of the Council's information systems have responsibilities in the event of a personal data breach. However, some have special responsibilities:

- **Corporate Management Team** - has overall responsibility for managing a personal data breach. It may not always be possible to obtain a Corporate Management Team decision to respond to a breach at short notice, in which case the Data Protection Officer (DPO) or Senior Information Risk Officer (SIRO) has the authority to act. This is in order to expedite any immediate action required to limit the level of risk to people's rights and freedoms and to satisfy the Council's obligations under GDPR;

- **Breach Lead** - is a temporary designation, assigned by Corporate Management Team to a senior manager on the detection of a breach. The Breach Lead will take a leading role in co-ordinating the breach response and will liaise closely throughout with the DPO, SIRO and Corporate Management Team;

- **Data Protection Officer (DPO)** - will assist the Breach Lead in assessing the level of risk to people's rights and freedoms. The DPO may make a decision to notify the ICO or the data subject in the absence of the SIRO, based on the outcome of any risk assessment. The DPO is normally the first point of contact with the Information Commissioner's Office and has a legal duty to cooperate with them;

- **Senior Information Risk Officer/Owner** (**SIRO)** - will assist the Breach Lead in assessing the level of risk to people's rights and freedoms. The SIRO may make a decision to notify the ICO or the data subject in the absence of the DPO, based on the outcome of any risk assessment;

- **Information Asset Owners** - the Council's Deputy Directors and Assistant Directors are responsible for the timely internal escalation of actual or potential personal data breaches (especially within their own service areas) to the DPO, SIRO and Corporate Management Team;
- **IT Services** - has responsibility for ensuring appropriate technical measures are in place to detect a breach of the Council's IT equipment or systems and for the timely reporting of actual or personal data breaches to the DPO and SIRO;
- **Information Governance Manager** - will provide advice and guidance to staff and elected Members and will take a leading role in reviewing and updating relevant policies and procedures;
- **All authorised users** - must promptly report any actual or potential personal data breach to their line manager, or the DPO, SIRO or IT Services (in the event of IT equipment or systems being compromised by a security incident).

7. 10 Step Plan - for Managing a Personal Data Breach

7.1 Step 1 - Breach detection

7.1.1 We will seek to put in place the necessary organisational and technical measures to detect a personal data breach. This will include providing appropriate training and awareness, contracts with processors and breach detection software and/or hardware system alerts.

7.1.2 If one of our processors detects a breach affecting personal data processed on behalf of the Council, they have a legal duty under GDPR to inform us without undue delay, as soon as they become aware. This requirement will be written into our contracts with processors.

7.2 Step 2 - Internal notification and escalation

7.2.1 All of the Council's authorised users are required to provide internal notification of an actual or potential personal data breach, immediately on detection. The procedure for this is set out in the Personal Data Breach Response Protocol and Internal Data Breach Notification Form.

7.2.2 Information Asset Owners have particular responsibility for escalating actual or potential personal data breaches within their own service areas, to the DPO, SIRO and Corporate Management Team.

7.3 Step 3 - Breach Lead and resources

7.3.1 Corporate Management Team will assign a senior manager as 'Breach Lead,' whose responsibility it will be to investigate the breach, co-ordinate activity for containment or recovery, assess risk, liaise with the DPO and report progress to Corporate Management Team.

7.3.2 Corporate Management Team will provide the Breach Lead at the earliest opportunity with the resources required to undertake the necessary breach response.

7.3.3 The Breach Lead will have responsibility for assessing the level of risk to people's rights and freedoms, with the assistance of the DPO and/or SIRO.

7.3.4 Information about the designation and role of the Breach Lead and how to contact and liaise with them will be communicated by Corporate Management Team to all relevant authorised users.

7.4 Step 4 - Containment and recovery

7.4.1 The aim of this stage is to contain the situation as quickly as possible and prevent it from getting worse or happening again.

7.4.2 On becoming aware of a personal data breach, we will take immediate action to contain a breach and to limit any potential harmful consequences. In relation to the Council's IT systems, this may mean isolating or closing down any compromised sections of the network.

7.4.3 It may be that a breach cannot be immediately contained or recovered, in which case, an assessment of risk will be undertaken at an early stage, to establish what action is necessary to achieve successful containment or recovery.

7.4.4 Where a breach involves any form of theft or criminal activity, we will inform the Police at the earliest opportunity.

7.5 Step 5 - Assessing risk

7.5.1 Once we have taken any immediate measures to contain or recover a personal data breach, we will then establish the likelihood and severity of the resulting risk to people's rights and freedoms. In carrying out an assessment of risk, we will take account of Recital 85 of GDPR and of the range of potential negative consequences of a breach on individuals, including emotional distress and physical and material damage.

7.5.2 In assessing risk to individuals, we will pay particular attention to any sensitive personal data (special categories) which may be affected by a breach.

7.6 Step 6 - Notifying the Information Commissioner's Office (ICO)

7.6.1 Having carried out a risk assessment, we will notify the ICO if it is likely that there will be a risk to people's rights and freedoms. In which case, we will report a breach to the ICO without undue delay and not later than 72 hours after becoming aware of it, in accordance with the ICO's data breach reporting guidance and procedures. If for some reason it takes longer than 72 hours, we will provide the ICO with reasons for the delay.

7.6.2 If it is not possible for us to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it, we will provide the required information to the ICO in phases, without undue delay.

7.6.3 The decision to notify the ICO will be considered on a case by case basis. Not all breaches will need to be reported to the ICO. Following a risk assessment, if it is considered likely there will be a risk then we will notify the ICO. If it is unlikely, then we will not report it, although we will record it in our Personal Data Breach Incident Log.

7.7 Step 7 - Communicating with the data subject

7.7.1 In the event that a risk assessment establishes that a breach is likely to result in a high risk of adversely affecting peoples' rights and freedoms, we will seek to inform those individuals without undue delay.

7.7.2 We will describe to individuals in clear and plain language, the nature of the personal data breach, the name and contact details of our DPO, the likely consequences of the breach and a description of the measures taken, or proposed to be taken, to mitigate any possible adverse effects.

7.7.3 In the event of a public communication, or similar measure, the Council's Communication Officer will be consulted on appropriate communication methods.

7.8 Step 8 - Investigation

7.8.1 Corporate Management Team will determine a plan of action, timescales and reporting relating to any breach investigation, to be instigated by the 'Breach Lead.'

7.8.2 We will investigate whether or not the breach was a result of human error or a systemic issue and how a recurrence can be prevented, whether through improved processes, further training or other corrective steps.

7.8.3 To inform the evaluation process, the Breach Lead will produce a final investigation report, to be presented to Corporate Management Team at the earliest opportunity following completion of the breach response and may also be required to provide interim reports.

7.9 Step 9 - Recording

7.9.1 We will record all personal data breaches and related decision-making processes in line with the requirements of the accountability principle, regardless of whether we are required to notify the ICO or data subjects. This is so that we can capture and measure the severity of breaches and near misses and also to justify any reasons for not notifying a breach.

7.9.2 We will record all actual or potential breaches in a Personal Data Breach Incident Log, which will be available for inspection by the ICO whenever required. We will document the facts relating to a breach or potential breach, its effects and any remedial action taken and will retain the log as a permanent record.

7.10 Step 10 - Evaluation

7.10.1 Once a breach response has been completed, we will investigate the causes of it and evaluate the effectiveness of the response. We will seek to implement any improvements and controls as soon as possible and communicate them to all relevant authorised users.

8. Compliance

8.1 Failure to comply with this policy may result in financial loss or reputational harm to individuals, businesses, organisations and the Council.

8.2 Any violation of this policy will be investigated and may lead to disciplinary action (for a member of staff), or to a Member being referred to Accounts and Governance Committee. A violation by a contractor, partner or agent will be addressed through the terms of the relevant contract.

8.3 In any situation where an authorised user is uncertain whether a security incident constitutes a personal breach, they should seek guidance from their line manager, the DPO, the SIRO, or IT Services (in the event of IT equipment or systems being compromised by a security incident).

9. Review

9.1 This Personal Data Breach Policy will be reviewed in April 2020 and annually thereafter, by the Information Governance Manager, DPO and the SIRO and updated as required.