STROUD DISTRICT COUNCIL
www.stroud.gov.uk

Data Breach Policy

February 2021

Corporate Policy & Governance

Last updated: 11/05/2021

Next document review by: 01/02/2022

Reviewed by: Marie Parkington, Corporate Policy & Governance

Approved by: *Name or Committee*

Amendment History

New Version Number	Issued By	Nature of amendment	Approved by & Date	Date on Intranet
0.1	Information Governance Officer	First Draft for comments	Marie Parkington	01/03/2021
1.0	Information Governance Officer	Appendix 1 for severe /critical breaches added	Marie Parkington	

1. Scope

1.1 This policy extends to all employees, contractors, agents, consultants, partners or other persons engaged in the council's service delivery, together with and elected members (in terms of information received, created or held by an elected member on behalf of the council)

2. Purpose

2.1 To have a standardised management approach throughout the council in the event of a serious security incident or data breach by having clear policies and procedures in place. Fostering a culture of proactive reporting and logging to maximise the potential for incidents and/or breaches to be identified and addressed.

2.2 Incident management is the process of handling incidents and breaches in a controlled way ensuring they are dealt with efficiently, with a consistent approach to ensure that any damage is kept to a minimum and the likelihood of recurrence is reduced by measures taken.

3. Introduction

3.1 Stroud District Council is responsible for the security and integrity of all information it holds. The Council must protect this information using all means necessary by ensuring at all times that any near miss or actual incident which could cause damage to the Council's assets and reputation is prevented and/or minimised as well as damage or distress to the data subject.

3.2 A personal data breach is defined 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." A breach is a type of security incident, however, the GDPR only applies where there is a breach of personal data. Near misses, are any kind of breach which could have occurred but was prevented by early intervention.

4. Breach Categories

4.1 Confidentiality Breach

A breach of confidentiality is when data or private information is disclosed to a third party without the data owner's consent. Whether an intentional breach, accidental error or theft, the data owner may be entitled to take legal action for potential losses or damage that comes as a result of the breach of confidentiality

4.2 Integrity Breach

An integrity breach is where there is an unauthorised or accidental alteration of personal data

4.3 Availability Breach

An availability breach where there is an accidental or unauthorised loss of access to, or destruction of, personal data

5. Reporting Breaches

5.1 This section is about reporting all security incidents and data breaches, classifying the incident and taking appropriate mitigating action.

5.2 The individual who discovers or receives a report of a security incident must complete our Data Breach Notification Form which can be found on our website and The Hub - under Information Governance.

5.2.1 This form can be used by internal members of staff, a supplier - processing data on behalf of the Council, or a member of the public who is concerned about a breach.

5.2.2 All suppliers or organisations processing data on behalf of Stroud District Council will be legally required to notify of a breach involving Council data.

5.3 If the incident occurs or is discovered outside normal working hours, this should be done as soon as practically possible. Reported breaches may need to be reported to the Information Commissioner's Office by the Data Protection Officer within a 72-hour timeframe therefore, it is important to report all incidents as soon as possible in order that an early assessment can be made.

5.4 Details of security incidents can be very sensitive and any sensitive information must be handled with discretion and only disclosed to those who need to know the details.

5.5 Employees or others working on behalf of the council must not attempt to deal with a security incident other than reporting the incident using the Data Breach Notification Form. Where action needs to be made immediately, this must be passed to the Data Protection Officer or Information Governance Officer (IGO) in the DPO's absence, as soon as possible.

5.6 The DPO/IGO will determine whether it is a security incident or data breach and will allocate it in accordance with the appropriate management plan. Employees must not attempt to conduct their

own investigations, unless specifically authorised to do so by the DPO / IGO – this does not apply to gathering of the relevant facts.

5.7 The council's Data Protection Officer is ultimately responsible for leading the management plan for the breach in question and making any decisions, in conjunction with the Senior Information Risk Officer (SIRO) about notification of the incident to the Information Commissioner's Office (ICO).

6. Data Breach Management Plan

6.1 The Data Protection Officer will lead all data breach investigations and will follow the Information Commissioner's Office (ICO) suggested Breach Management Plan: -

- Containment and recovery.
- Assessment of ongoing risk.
- Notification of breach.
- Evaluation and response.

6.2 **Containment and Recovery**

6.2.1 Containment and recovery involves limiting the scope and impact of the data breach, and stemming it as quickly as possible.

6.2.2 All Data Breach Notification Forms will be directed to the Data Protection Officer (DPO). The DPO, or IGO in the DPO's absence, will consider the breach and the most appropriate course of action, including practical steps such as who should contact whom, both inside and outside the Council.

6.2.3 From the time that the DPO/IGO is made aware of the breach, they will have 72 hours to investigate whether the breach represents a risk to the Rights and Freedoms of individuals, and therefore whether it should be reported to the ICO.

6.2.4 The DPO/IGO will work with the manager for the service area affected and together they will take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include: -

- Informing individuals that they have been affected by a breach
- Attempting to recover any lost equipment or personal information.
- Shutting down an IT system or remotely wiping lost devices
- Contacting the Communications Team where appropriate dependent on the nature of the breach so they can be prepared to handle any press enquiries or to make any press releases.
- The use of backups to restore lost, damaged or stolen information.
- If bank details have been lost/stolen consider contacting banks directly for advice on preventing fraudulent use.

● Making a building secure

● If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

6.2.5 The investigation should consider: -

●The type of information or equipment affected

● The category and sensitivity of the information

● How many individuals are affected by the breach? How many records are affected?

● What protections are in place (e.g. encryption)?

● What happened to the information?

● Whether the information could be put to any illegal or inappropriate use.

● What could the information tell a third party about the individual?

● What types of people have been affected (the public, suppliers, staff etc.)?

● Whether there are wider consequences to the breach.

6.2.6 The DPO/IGO will record the findings and any resultant action plan on the Data Breach Investigation Form. This will be shared with the service area manager and any actions monitored.

6.3 **Assessment of Ongoing Risk**

6.3.1 Following a breach, it is essential as part of the management plan, that the manager assesses the risks arising from the breach and if they are likely to reoccur. The DPO/IGO can offer advice and support with process.

6.3.2 The manager will ascertain what information was involved in the breach, what led to the breach and what action can be taken to prevent the breach from reoccurring, including refreshing staff training, and making immediate improvements to processes which are vulnerable to a breach.

6.4 **Notification to Information Commissioner's Office**

6.4.1 If the data breach is likely to result in a high risk to the rights and freedoms of individuals, then it is mandatory to notify the ICO without undue delay, and within 72 hours of being made aware of the breach.

6.4.2 Every incident will be considered on a case-by-case basis and the decision to report to the ICO will be determined by carrying out a risk assessment. The DPO/IGO will assess the risks of each case using the methodology recommended by the ICO, and developed by The European Union Agency for Network and Information Security (ENISA). The methodology gives a score which calculates the severity of a breach using the following formula:

Severity = DPC x EI + CB

Data Processing Context (DPC) - addresses the type of data involved in the breach, together with a number of factors linked to the overall context and use of processing.

Ease of Identification (EI) - Determines how easily the identity of the individual can be deduced from the data involved in the breach

Circumstances of breach (CB) - Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breach data, as well as any involved malicious intent.

In this way, in order for the DPO to get the severity result, all three criteria should be scored. The result belongs to a certain range of values which corresponds to one of the four severity levels: low, medium, high and very high. At the end of the assessment, other possibly relevant criteria (number of individuals and unintelligibility of data) that have not been considered in the methodology are evaluated and flagged to the competent authority when applicable.

For detailed information on the scoring of the criteria, follow the steps contained in section 3.1 of the Data Breach Notification Tool

Additional points will be added based on the volume of individuals affected - using the following scale:

Additional Score	Description of volume of individuals affected
0	Information about 10 or less individuals
1	Information about 11-100 individuals
2	Information about 101-1,000 individuals
3	Information about 1,001 and over individuals

The scores will then be collated and used to determine an overall rating of risk from low to very high. Risks which are high or very high will require notification to the ICO.

SEVERITY RATING ASSESSMENT		
SE < 2	**Low**	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spend re-entering information, annoyances, irritations etc)
2 ≤ SE < 3	**Medium**	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments etc)
3 ≤ SE < 4	**High**	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, worsening of health etc)
4 ≤ SE	**Very High**	Individuals may encounter significant, or even irreversible consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death etc)

6.4.3 All high or very high risk incidents must be communicated directly to the affected individuals by the Information Governance Officer without undue delay. When notifying individuals, communication must be in clear and plain language, and at least provide:

● A description of the nature of the breach;

● The name and contact details of the Data Protection Officer;

● A description of the Council's assessment of the likely consequences of the breach; and

● A description of the measures taken or proposed to be taken by the Council to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.4.4 Communication to affected individuals is not required under the following conditions;

● If technical and organisational measures have been taken i.e. encryption, or;

● There is disproportionate effort involved i.e. if the contact details of the individuals affected is not known or if the individuals cannot be easily identified. In the case of disproportionate effort and in appropriate cases as decided by the DPO, data subjects must be informed in an equally effective manner, i.e. public announcement.

6.4.5 The Data Protection Officer will make the final decision regarding communication to individuals and escalation of an incident to the ICO. These actions must not be taken by anyone else, unless directed to do so by the Data Protection Officer.

6.4.6 When the Council is not in a position to notify a breach to the ICO within 72 hours after becoming aware of it, the Council must be able to provide reasons for this delay - to ensure it is justified and not excessive. The timeliness of reporting breaches is therefore an essential aspect of

compliance. In these circumstances, the DPO will inform the ICO of a potential reference and give reasons for any potential delay. e.g., relevant officers on leave

6.5 **Review and Evaluation**

6.5.1 Once the initial impact of the breach is over, the DPO/IGO should fully review both the causes of the breach and the effectiveness of the response to it, and where appropriate, work with Internal Audit, Senior Information Risk Owner (SIRO), and other relevant Officers to determine if any further control improvements are required.

6.5.2 The DPO/IGO will follow up with the service area following a breach, to discuss the causes of the breach and monitor that any necessary changes identified in the breach management plan are implemented in a timely manner.

6.5.3 The DPO / IGO will record all data breaches on a central record where reported to the ICO or not and will provide annual update reports to Strategic Leadership Team and Audit and Standards Committee.

7. Training and Awareness

7.1 All staff must complete the Data Protection course annually and managers are responsible for ensuring that their staff do so. The training provides learning on our responsibilities under the General Data Protection Act, in regard to protecting the data we hold and the systems we use.

7.2 All Information Asset Owners/Managers must also read the Information Governance Framework and associated policies, mentioned therein on an annual basis.

8. Implementation

8.1 This policy is effective immediately.