Ref. No.	CO/IG/10
Category:	
People	
Place	
Corporate	Yes
In Constitution	

Data Breach Policy

Policy Details

What is this policy for?	The Data Breach Policy describes how the Council will manage and respond to personal data breaches in accordance with data protection law.
Who does this policy affect?	All members, employees, students, apprentices, volunteers, contractors and other third parties handling council information
Keywords	Personal data breach, data breach
Author	Alison Richmond, Data Protection Officer
Dorset Council policy adopted from	This is a new policy for Dorset Council, which supersedes any previous sovereign councils' policies in relation to personal data breaches.
Does this policy relate to any laws?	Data Protection Act 2018; General Data Protection Regulation (GDPR)
Is this policy linked to any other Dorset Council policies?	This policy is part of the Information Governance Framework, which also includes: • Data Protection Policy • Data Protection Impact Assessment Policy • Data Protection Policy • Individual Rights Policy • Confidential Waste, Clear Desk and Screen Policy • Data Quality Policy • Protective Marking Policy • Records Management Policy • Records Retention Policy • Information Security Management Policy and related standards and protocols
Equality Impact Assessment (EqIA)	An EqIA screening tool was completed and submitted on 26th March 2019. The tool identified that there was no need to complete an EqIA.
Other Impact Assessments	N/A

Status and Approvals

Status	Live	Version	1
Last review date	This is a new policy	Next review date	1 April 2020
Approved by (Director)	Dorset Council Corporate Director, Legal and Democratic	Date approved	February 2019
Member/ Partnership Board Approval		Date approved	

Data Breach Policy

Purpose	This policy sets out Dorset Council's approach to complying with it's responsibilities to record, manage and report data breaches, as well as important roles and responsibilities, as set out by the General Data Protection Regulation (GPDR), Data Protection Act 2018 (DPA) and other laws that regulate how personal data is managed.
Scope	The Data Protection Breach policy forms part of the overarching Information Governance Framework. This policy covers all personal and special category data breaches for which the Council is the Data Controller. When the Council is the Data Processor, this policy must be referred to in conjunction with the relevant contract and/or data sharing agreement. This policy applies to all members, employees, agency staff, students, apprentices, volunteers, contractors and other third parties handling the Council's personal data. The policy supplements our other Governance policies. We may add or amend to this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted. Our Data Protection Officer has overall responsibility for the day to day implementation of this policy.

Table of contents

1. Introduction

1.1. The General Data Protection Regulation (GDPR) outlines a data breach as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to, personal data.

1.2. The Dorset Council therefore has a legal responsibility to ensure that personal data held by the Council is safeguarded and failing to do this could result in personal data being compromised and a data breach occurring.

1.3. Depending on the nature and severity, a data breach could cause physical, emotional or non- material damage to affected individuals.

1.4. Failure to notify a breach, when required to do so, can result in a significant fine up to 10 million euros. The fine can be combined with the ICO's other corrective powers and thus every effort must be made to prevent data breaches.

2. Data in scope

2.1. Personal data is information from which living individuals can be identified by anyone, whether directly or indirectly, by all means likely to be used. It is information about someone whose identity is apparent, or can be reasonably ascertained, from the information or a combination of information from different sources. Examples of personal data processed within the Council includes:

- Name and addresses;
- Contact details;
- Medical or bank details;
- Combination of identification elements such as physical characteristics pseudonyms occupation, address etc.;
- Online Identifier such as people's IP address;
- Personal data includes indirect information that can be used to ascertain someone identify e.g.
  - Physiological data;
  - Genetic information;
  - Social data;
  - Financial information.

The above list is not exhaustive; however, it is important to consider the different types of information from which a person can be identified and to take all necessary steps to protect it in accordance with legal requirements.

2.2. Special category data is personal information which is more sensitive in nature and may result in harm, distress or discrimination to an individual if it was compromised. Examples of special category data processed within the Council includes:

- Race;
- Ethnic origin;
- Political or religious affiliations or beliefs;

- Trade union memberships;
- Genetic Information;
- Biometrics data;
- Health information;
- Sex life; or
- Sexual orientation.

2.3. A personal data breach includes but is not limited to the following:

- Unauthorised access to systems (manual or electronic) containing personal data.
- Sending personal data to an incorrect or unauthorised recipient(s) (hardcopy or electronic).
- Loss of personal data (paper or electronic) and thus making it unavailable
- Losing devices, which have means of accessing data including laptops, USB sticks, mobile phones. ALL lost and stolen devices must be reported to IT without delay.
- Altering personal data without permission.
- Hacking of IT systems, resulting in the loss of authentication credentials such as passwords.
- Disposing of personal data incorrectly (confidential waste etc)
- Collecting or using personal data without a lawful basis (please see relevant IAR)
- Attempts (failed or successful) to gain unauthorised access to personal data or systems containing personal data.

3. Data breach objectives

3.1. Dorset Council will record all breaches, regardless of whether or not they need to be reported to the ICO.

3.2. The GDPR outlines mandatory requirements to report high risk/potentially damaging data breaches to the Information Commissioner's Office (ICO) within 72 hours. Depending on the circumstance, affected individuals may also have to be notified.

3.3. In these circumstances, the SIRO will also be notified due to the identification of a new information risk.

3.4. The general responsibility for breach mitigation actions will lie with the team responsible/relevant manager, with advice and directions given by the Data Protection Team and information governance staff.

3.5. The severity of a breach will be graded according to the significance of the breach and the likelihood of those serious consequences occurring, using NHS guidance where appropriate.

3.6. Severity of harm to the individuals whose personal data is affected by the data breach will be judged on a case by case basis by the most appropriate individual involved i.e. Data Protection Team (DPO), other professionals etc.

4. Roles and responsibilities

4.1. Everyone processing personal data is responsible for adhering to this data breach policy. It is essential to report all data breaches to the Data Protection Team, so that they can be thoroughly investigated. If in doubt, still report it.

4.2. All information users (controllers and processors) with access to Council information are responsible for:

- Staff (including temporary employees, contractors, consultants and volunteers):
  - Complying with this policy when processing personal data in the performance of their duties.
  - Knowing how to recognise a data breach and reporting it to the Data Protection Team accordingly.
  - Fully cooperating and assisting when required, especially when urgent action needs to be taken to mitigate damage.
  - Failure to adhere to this policy may result in disciplinary action for individuals, and enforcement action, financial loss and/or reputational damage to the Council.
- Managers:
  - Ensuring staff in their area act in compliance with this policy.
  - Have sufficient training and awareness of procedures in place, to deal with data breaches effectively.
  - Assisting and investigating data breaches as required, especially when risk is high.
- DPO:
  - Overseeing management of complex breaches.
  - Delegating responsibility where appropriate.
  - Being the first point of contact with the ICO and reporting breaches should they meet the risk threshold.
  - Preventing data breaches; investigating the causes of data breaches and making recommendations to apply any learning.
  - Reporting breaches involving NHS data via the Data Security and Protection Toolkit (DSPT)
- Data protection and Information governance teams:
  - Assisting the DPO and managers with data breach investigations
- Information Asset Owners:
  - Ensuring prevention/mitigation plans are in place to prevent reoccurrence of data breaches affecting their information assets
  - Sharing lessons learnt from data breaches with users of their assets and other IAOs

- SIRO:
  - Advising the Chief Executive or relevant accounting officer on information breaches
  - Ensuring prevention/mitigation plans are in place to protect personal data should a high-risk breach occur or one that affects multiple information assets.
  - Information risk management within the Council including any resolution of escalated risk issues raised by Information Asset Owners; IT Officers etc.

5. Related policies

5.1. Please see the intranet for related policies, including Data Protection Policy

6. Monitoring and Review

6.1. This policy will be subject to annual review by the DPO/SIRO and MO

7. Associated Legislation

7.1. The GDPR Articles 33 & 34

7.2. European Convention on Human Rights Article 8

7.3. The Data Protection Act 2018

7.4. Common Law Duty of Confidentiality

Glossary

Personal data *– information that can be used, directly or indirectly, to identify a living individual. That information can be held in a variety of formats, storage media and locations. For example, fields in a database, CCTV footage, or paper files in a filing cabinet.*

Special Category Data *– is data that includes racial or ethnic origin, political opinions, religious or philosophical beliefs, Trades Union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, health, sex life or sexual orientation. The processing or data relating to criminal convictions also requires special category treatment.*

Processing *- any action involving data. For example, collecting, recording, holding, using, disclosing, erasing etc.*

Data Controller *– a controller determines the purposes and means of processing personal data*

Data Processor *– a processor is responsible for processing personal data on behalf of a controller*

IAR *– An Information Asset Register is used by the Council to manage information assets and potential risks. It is also used to record the reasons / legal bases relied upon to hold/process personal data.*

SIRO *- Senior Information Risk Officer.*