Ref. No.	CO/IG/4
Category:	
People	
Place	
Corporate	Yes
In Constitution	

Data Protection Policy

Policy Details

What is this policy for?	This policy sets out Dorset Council's approach to complying with the General Data Protection Regulation, Data Protection Act 2018 and other laws that regulate how personal data is managed
Who does this policy affect?	All members, employees, students, apprentices, volunteers, contractors and other third parties handling personal data
Keywords	Personal data, personal information, special category data, sensitive personal data
Author	Kate Watson, Information Governance Officer, Dorset Councils Partnership.
Dorset Council policy adopted from	New policy for Dorset Council, which supersedes the below sovereign councils' policies: • Christchurch and East Dorset Councils Personal Data and Security Incident Reporting • Dorset County Council Data Protection Policy • Dorset Councils Partnership Data Breach Policy • Purbeck District Council Reporting 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: • Information Governance Policy • Data Breach Policy • Individual Rights Policy • Data Protection Impact Assessment (DPIA) 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 5th 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	1.0
Last review date	This is a new policy	Next review date	1 April 2020
Approved by (Director)	Dorset Council Corporate Director: Legal & Democratic	Date approved	February 2019
Member/ Partnership Board Approval		Date approved	

Shadow Dorset Council

Data Protection Policy

Purpose	*This policy sets out Dorset Council's approach to complying with the General Data Protection Regulation (GPDR), Data Protection Act 2018 (DPA) and other laws that regulate how personal data is managed.*
Scope	*Data Protection is a part of the overarching Information Governance Framework, which describes how personal, confidential and corporate information is managed by Dorset Council.* *This policy covers all personal data 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, students, apprentices, volunteers, contractors and other third parties handling personal data.*

Table of contents

Shadow Dorset Council

1. Introduction

1.1. The General Data Protection Regulation (GPDR) and Data Protection Act 2018 (DPA) regulate how personal data relating to living individuals is managed.

1.2. Dorset Council will process personal data relating to local residents, service users, customers, current, past and prospective employees, clients and suppliers in accordance with the requirements of the GDPR, DPA, common law duty of confidentiality and other relevant legislation e.g. the Human Rights Act 1998.

2. Data protection principles

2.1. The Council's data protection activities will be designed to meet the requirements of the GDPR Accountability principle. All processing of personal data will be tailored in a way that respects the data protection principles set out in the GDPR and evidence must be kept of how the Council complies with these principles:

- Personal data processing must be lawful and transparent, ensuring fairness towards the individuals whose personal data is being processing ('lawfulness, fairness and transparency')
- Specific purposes must be identified for processing personal data and individuals must be told of these when collecting their data. Personal data cannot be used for other purposes that aren't compatible with this original purpose ('purpose limitation')
- Only the personal data necessary to fulfil that purpose must be collected ('data minimisation').
- Personal data must be kept accurate and up-to-date, and corrected if it is found to be inaccurate for its intended purpose ('accuracy').
- Personal data must not be stored for longer than necessary for the purposes for which it was collected ('storage limitation')
- Appropriate technical and organisational safeguards that ensure the security of the personal data must be put in place, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology ('integrity and confidentiality')

3. Data protection objectives

3.1. To comply with data protection legislation, the Council will ensure so far as practicable that:

- The annual data protection fee will be paid to the Information Commissioner's Office (ICO) on behalf of Dorset Council and every member who attends information governance training
- Adequate security measures are implemented to protect personal data
- Documentation is maintained about processing activities, including the source of personal data, lawful basis, and sharing agreements, within the Council's Information Asset Register
- Training needs are assessed and training is provided to all staff processing personal data, about which training records are kept
- Staff are aware of where they can find data protection advice
- Data protection policies and associated procedures are adopted and regularly reviewed
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of special categories of personal data will be in compliance with approved procedures
- Written contracts, containing the terms specified by the GDPR, are put in place with organisations that process personal data on the Council's behalf (Data Processors)

- Procedures are put in place to allow data subjects to fully exercise their rights under GDPR and DPA
- Personal data breaches are recorded and, where necessary, are reported [see Data Breach Policy and Data Breach Procedure]
- A 'data protection by design and default' approach is taken, with data protection integrated in organisational design and project management at the design phase of any new process, procurement or creation of a new information asset or new ways of using existing data
- Data Protection Impact Assessments (DPIAs) are carried out for relevant projects, especially those using new and emerging technologies, or existing technologies in new ways that are likely to pose a risk to the right and freedoms of individuals. DPIAs that are found to have a medium or high risk will be reviewed by data protection subject matter experts.

4. Roles and responsibilities

4.1. Everyone collecting, using, storing and disposing of personal data is responsible for following good data protection practice.

4.2. All information users with access to Council information are responsible for:

- Members
  - Complying with this policy when acting as a Member of the Council e.g. sitting on a committee
  - Note: when acting as a representative of residents of their ward Members are individually responsible for the processing of personal data.
- Employees (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 personal data breach and reporting data breaches, or suspected breaches, as described in the Data Breach Policy.
  - 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
  - Implementing data protection policies and procedures within their areas

4.3. Some roles have specific responsibilities:

- Senior Information Risk Owner (SIRO)
  - Overseeing the development of data protection policy and strategy within the overall information governance framework
- Caldicott Guardian
  - Inputting into the development of data protection policy and procedures, with a particular focus on the storage, handling and sharing of personal information relating to patients, service users and their care.
- Data Protection Officer (DPO)
  - The DPO is an individual designated for the purposes of the GDPR, responsible for helping the council fulfil its data protection obligations. Key responsibilities are described in the Information Governance Policy. These include maintaining this policy and associated procedures, monitoring compliance with data protection legislation, awareness-raising, training, and audits.
- Information Asset Owners (IAOs)
  - Ensuring that information assets containing personal information are managed according to data protection policies and procedures

- Keeping records of personal data processing in Information Asset Register entries up-to-date
- Negotiating, managing and approving agreements on the sharing of their information assets containing personal information
- Monitoring and addressing potential risks to compliance with this policy, for example the risks of a legacy system storing records becoming unusable

5. Training

5.1. Dorset Council will provide data protection training to all Council information users.

5.2. All employees must complete mandatory data protection training at induction and annually. Enhanced training will be provided to high-risk users (e.g. front line staff, those working with NHS data, joint teams working in hospitals) as prescribed by the organisation.

5.3. Data protection professionals should receive specialist training relevant to their role.

5.4. Awareness sessions will be provided to teams on request and regular reminders on data protection topics made available through corporate communication channels.

6. Related policies

6.1. See the Information Governance Policy for a list of all the policies that make up Dorset Council's Information Governance Framework.

6.2. Related policies and procedures to this Data Protection Policy include:

- Data Breach Policy and Procedure
- Individual Rights Policy
- Subject Access Requests Procedure
- Data Protection Impact Assessment Policy and Procedure
- Confidential Waste, Clear Desk & Screen Policy

7. Monitoring and review

7.1. Monitoring of this policy will be led by the Data Protection Officer on a regular basis and reported to the Information Governance Board. This policy will be reviewed annually to ensure it continues to meet the requirements of the Council and the current legislation.

Annex A – 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.

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

Data breach – breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

DPIA - Data Protection Impact Assessment (DPIA), a process to help identify and minimise the data protection risks of a project

Information Asset Register (IAR) – a mechanism for understanding and managing the Council's information assets, their risks and business requirements