ADUR & WORTHING
COUNCILS

Data Protection Policy

Document Control

Author	Senior Information Governance Officer
Current Version	3.0
Implementation Status	Approved / Implemented
Approved by	Joint Officer Negotiating Group (JONG)
Date of Publication	13/05/2020
Distribution	All staff and public website
Review Date	June 2021

ADUR & WORTHING
COUNCILS

1. Purpose

The purpose of this policy is to ensure appropriate measures are applied by the Adur & Worthing Councils to comply with the data protection legislation, namely, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), as well as the Information Commissioner's Office (ICO) guidance.

2. Scope

The Councils are committed to compliance with all data protection legislation in respect of personal data and the protection of the rights and freedoms of individuals whose information the Councils collect and process.

This policy applies to all staff, elected members, contractors and any other persons who have access to the Councils' information, information systems and networks.

This policy applies to all personal data processed, i.e. held, created, modified, accessed or shared, from the effective date of this policy. It includes personal data in any form, no matter whether it is stationary (e.g. an electronic or paper document) or in transit (e.g. file transfer, email, fax, phone, post). It also covers the Councils' buildings, premises and systems which contain that data.

3. Policy Statement

The policy sets out the Councils' commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data. The Councils are committed to:

- Ensuring that we comply with the data protection principles;
- Meeting our legal obligations as laid down by the data protection law;
- Ensuring that personal data is collected and used fairly and lawfully;
- Processing personal data only where necessary in order to meet our operational needs or fulfil legal requirements;
- Taking steps to ensure that personal data is up to date and accurate;
- Establishing appropriate retention periods for personal data;
- Ensuring that data subjects' rights can be appropriately exercised;
- Providing adequate security measures to protect personal data;

- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues;
- Ensuring that all staff and Members are made aware of good practice in data protection;
- Providing adequate training for all staff and Members responsible for personal data;
- Ensuring that everyone handling personal data knows where to find further guidance;
- Ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly;
- Regularly reviewing data protection procedures and guidelines within the organisation.

4. Data Subjects' Rights

Data Subjects have the following information rights with regards to the Councils processing their personal data, subject to any exemptions or exceptions:

- To be informed about the collection and use of their personal data;
- To access and obtain a copy of their personal data;
- To withdraw any consent(s) given for processing at any time;
- To have personal data erased in certain circumstances;
- To request the restriction or suppression of processing in certain circumstances;
- To obtain and reuse their personal data for their own purposes across different services in certain circumstances;
- To prevent processing for purposes of direct marketing;
- To object to the processing of their personal data in certain circumstances;
- To not have significant decisions that will affect them taken solely by automated process unless in certain circumstances;
- To seek remedy in a court of law if they suffer damage by any contravention of the GDPR and/or the DPA;
- To request the supervisory authority (ICO) to assess whether any provision of the

GDPR and/or the DPA has been contravened.

5. Responsibilities

This section should be read in conjunction with the responsibilities detailed in Councils' other Information Governance and Security Policies. Additional responsibilities arising from this policy are specified below.

5.1 Data Protection Officer

A suitably qualified and experienced Data Protection Officer will be appointed to undertake their statutory duties:

- to inform and advise the Councils and employees about their legal obligations under the GDPR and DPA and other data protection laws;
- to monitor compliance with the GDPR and DPA and other data protection laws, and with the Councils' data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, Data Protection Impact Assessments;
- to cooperate with the Information Commissioner's Office;
- to be the first point of contact for the ICO.

In addition the Data Protection Officer will be responsible for:

- Keeping a central catalogue of service areas' Registers of Processing Activities;
- Manage and report as appropriate any personal data breaches;
- Advise the Councils on Privacy By Design;
- Annual renewal of notification ICO registration.

5.2 Senior Information Risk Officer

Is responsible for oversight of compliance and risk management.

5.3 CEO and Directors

The CEO and Directors are ultimately responsible for overseeing and ensuring compliance with this policy and data protection legislation.

Directors are responsible for ensuring that their respective Services are complying with the data protection legislation and that relevant data protection and information governance and security policies and procedures are enforced.

5.4 Heads of Service and Service Managers

It is the responsibility of Managers to ensure compliance with this policy within their own Service areas. Their responsibility includes:

- Ensuring that staff are aware of their responsibilities under the data protection legislation and follow information governance best practice;
- Ensuring employees, including contractors, consultants and volunteers employed to undertake Council business follow the Data Protection Policy and procedures;
- Ensuring that compliant contracts with Data Processors are in place;
- Ensuring that service areas' Registers of Processing Activities are maintained and updated regularly;
- Ensuring that service areas' Privacy Notices are maintained and updated regularly;
- Ensuring that service areas' Information Retention and Disposal Schedules are maintained and updated regularly;
- Ensure appropriate resources are in place to enable compliance with the Data Protection Policy;
- Ensure that compliance with data protection legislation under the DPA, GDPR, any other data protection legislation and good practice can be demonstrated.

5.5 Staff

All staff:

- Must be aware of the data protection legislation and of their obligations under it;

- Individual staff members may be personally liable for privacy breaches if they act outside the authority of the data controller;
- All new members of staff must undertake data protection training and familiarise themselves with the Councils' Data Protection Policy and procedures as part of their induction process and in training sessions provided by the Councils;
- Refresher training will be carried out for all staff on a regular basis, in particular when there are any changes in legislation, when there is a significant information security incident or on a yearly cycle at the Councils' discretion;
- Report personal data breaches to the Data Protection Officer as soon as possible.

5.6 Elected Members

All Elected Members:

- Should be made fully aware of this policy and of their duties and responsibilities under the data protection legislation;
- When handling personal data in their role as politicians (e.g. when out canvassing), Members should be complying with the rules and requirements of their respective political parties and their Data Protection Policies;
- When acting in their role as Elected Members, they should be complying with the Councils' Data Protection Policy. As such, they have to handle personal data in line with the requirements of the Councils' Data Protection Policy.

6. Complaints

All complaints regarding Councils' handling of Information Rights requests will be dealt with by the Data Protection Officer or an appropriate nominated Senior Officer. The Councils will make available details of the complaint procedure to applicants. Complaints will not be handled by persons who participated in the original decision.

Complaints and requests for review should be submitted by the applicants to the Data Protection Officer within three (3) months of receipt of the initial response.

Where the Councils' procedure upholds an initial decision, the applicant will be advised of the right to appeal and the steps involved to take the matter to the Information Commissioner.

7. Training associated with this Policy

Compulsory online training is provided to staff via Adur & Worthing E-Learning. Online training will also be provided to Members.

Additional workshops for staff and Members will also be organised by the Senior Information Governance Officer (SIGO) and the Information Officers (IO). Various guidance is available on the Intranet.

If anyone requires support, advice or guidance on any element outlined in this policy they should speak with their line manager in the first instance.

8. Monitoring

This Policy was consulted with the Unison and agreed by the Joint Officer Negotiating Group (JONG).

Compliance monitoring will be carried out by the Councils' Data Protection Officer and through the Councils' management structure.

Disciplinary action in accordance with procedures approved by the Councils may be taken against any employee who violates the requirements of this policy.

This Data Protection Policy will be reviewed annually by the Data Protection Officer.

9. Related documents

This policy should be read in conjunction with the following documents:

- Other policies in the Digital's Information Security Policy Suite;
- Any supporting standards, guidelines, processes and procedures.

ADUR & WORTHING
COUNCILS

10. Document History - Version Control

Version	Date	Notes/Reasons	Reviewers
2.1	April 2018	Unknown - history not recorded - ISPS-011	IS Project Team
3.0	06/02/2020	Policy updated to bring in line with current legislation. Formatting changed. Links & ref to JONG added. Responsibilities for SIRO, CEO and Senior Managers added. Members' responsibilities updated - requirement to register with the ICO removed. Complaints procedure added. Version Control table added.	SIGO
3.0	13/05/2020	Agreed by JONG. Finalised for publishing.	SIGO

ADUR & WORTHING
COUNCILS

Appendix A - Glossary

Personal data - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health (including mental health) or data concerning a natural person's sex life or sexual orientation.

Data Subject – an identified or identifiable natural person from the personal data held by an organisation.

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data breach – 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. There is an obligation on the Data Controller to report personal data breaches to the Information Commissioner's Office and where the breach is likely to result in a risk to people's rights and freedoms.