ADUR & WORTHING
COUNCILS

Data Protection Policy

Document Control

Author	Senior Information Governance Officer
Current Version	4.0
Implementation Status	Approved / Implemented
Approved by	
Date of Publication	13/05/2020
Distribution	All staff and public website
Last Reviewed Date	23/02/2022

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 UK General Data Protection Regulation (UK 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 fulfill 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. The Principles of Data Protection

The GDPR states that anyone processing personal data must comply with seven principles. These principles are legally enforceable.

The principles at Article 5(1) UK GDPR require that personal information:

1 Shall be processed lawfully, fairly and transparently

The Councils will:

- Ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful.
- Only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing.
- Ensure that data subjects receive full privacy information so that any processing of personal data is transparent.

2 Shall be processed specifically, explicitly and legitimately

The Councils will:

- Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice.

- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first.

3 Shall be adequate, relevant and not excessive

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- The Councils will only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.

4 Shall be accurate and kept up to date

- The Councils will ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.

5 Shall be kept for no longer than is necessary

- The Councils will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

6 Shall be processed in a manner that ensures appropriate security

- The Councils will ensure that there are appropriate organisational and technical measures in place to protect personal data.

7 The principle at Article 5(2) UK GDPR require that the Councils shall be able to demonstrate compliance with the above

The Councils will:

- ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request.

- carry out a Data Protection Impact Assessment (DPIA) for any high risk personal data processing, and consult the Information Commissioner if appropriate.
- ensure that a Data Protection Officer (DPO) is appointed to provide independent advice and monitoring of the Councils' personal data handling, and that this person has access to report to the highest management level of the Councils.
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law. The GDPR provides conditions for the processing of any personal data that must be met. It also makes a distinction between personal data, "special category" (sensitive) personal data and criminal conviction personal data. Special category personal data requires stricter conditions for processing.

5. 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 UK GDPR and/or the DPA;
- To request the supervisory authority (ICO) to assess whether any provision of the UK GDPR and/or the DPA has been contravened.

6. Transfers and Disclosures of Personal Data

In order to provide services and to meet our legal obligations as a local authority, the Councils will sometimes need to share your personal information with external organisations.

We will only share your personal information where it is necessary, either to comply with the law or where permitted under data protection legislation.

Examples of organisations, we may share your personal information with:

- NHS
- HMRC
- Police
- UK government departments, and related agencies
- other local authorities
- Ombudsmen, the ICO, the Care Inspectorate
- Care providers and voluntary organisations

For more information about who we share your personal data with and why, please see 'Service Related Privacy Notices' which can be found on the Councils' website.

The Councils only share your information with partners or contractors who agree, through Data Sharing/Processing Agreements, to protect your information.

Sharing information outside of the UK

Almost all personal data the Councils use is stored and processed in the UK. Some information may also be stored within the EU.

If we need to transfer your personal information outside of these areas for a particular activity, this will be explained in the relevant service-specific privacy notice together with a description of the protective measures we have put in place to keep it safe.

Any transfer of personal information between the Councils and partner organisations shall be carried out using a secure method agreed by the Councils' ICT Services.

7. Privacy Notices

The Councils shall ensure that a corporate privacy notice is published on the Councils' website. It shall explain in general terms:

- what information is being collected;
- why the Councils collect information;
- who the Councils may share this information with;
- what the Councils will do with the information;
- how long the Councils will keep the information;
- what rights individuals have
- how to contact the Councils' Data Protection Officer

  (data.protection@adur-worthing.gov.uk)
- how to contact the ICO

  by post at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or phone 0303 1231 113.
- You can also make a complaint or find out more information on the Commissioner's Office website.

Where relevant, service areas shall provide their own privacy notice(s) confirming this information in specific terms.

8. Register of Processing Activities (ROPA)

The Councils will:

- Record processing activities in electronic form so you can add, remove and amend information easily.
- Regularly reviews the record against processing activities, policies and procedures to ensure that it remains accurate and up to date, and you clearly assign responsibilities for doing this.
- Regularly review the processing activities and types of data you process for data minimisation purposes.

- Ensure that effective processes are in place to keep the record up to date, accurate and make sure that the data is minimised.
- Ensure that staff can explain their responsibilities and how they carry them out in practice
- The ROPA includes (as a minimum**)**
    - organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);
    - the purposes of the processing;
    - a description of the categories of individuals and of personal data;
    - the categories of recipients of personal data;
    - details of transfers to third countries, including a record of the transfer mechanism safeguards in place;
    - retention schedules; and
    - a description of the technical and organisational security measures in place.
- An internal record of all processing activities carried out by any processors on behalf of your organisation.

9. Data Security and Breach Management

The Councils shall ensure that it processes personal data securely by means of appropriate technical and organisational measures.

- These measures will include adherence with relevant Council policies
- Access to personal data shall be strictly controlled.
- The Councils shall investigate all suspected breaches which involve personal data.
- Where a breach is identified, this will be reported to the ICO where necessary, based on UK GDPR requirements.

10. Data Protection Impact Assessments

- A data protection impact assessment (DPIA) is a process to help the Councils identify and minimise the data protection risks of a project.

- The Councils will conduct a DPIA for major projects which require the processing of personal data or where processing is likely to result in a high risk to individuals' interests, rights and freedoms.

11. 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.

11.1 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 UK GDPR and DPA and other data protection laws;
- to monitor compliance with the UK 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 ICO;
- 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.

11.2 Senior Information Risk Owner

Is responsible for oversight of compliance and risk management.

11.3 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.

11.4 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, UK GDPR, any other data protection legislation and good practice can be demonstrated.

11.5 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.

11.6 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.

12. Contracts

- All Council contracts shall include appropriate terms to ensure that personal data is handled in accordance with the Data Protection Act 2018 and the UK GDPR.
- Personal data shall only be supplied for the agreed purposes as set out in the contract and shall not be used or disclosed for any other reason.
- The Councils shall ensure that before personal data is shared with a third party as part of a contract that appropriate technical and organisational security controls are

in place.

13. 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 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.

14. 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 Request for 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.

15. Monitoring

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.

16. 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.

17. Approval process for Data Protection Documentation

- In order to achieve and maintain control of documentation, any reviews and/or changes to data protection documentation (ROPAS/Privacy Notices/Retention and Disposal Schedules) may only be carried out and approved by the GDPR Lead or Head of Service within their own service block.
- (E.g. The GDPR Lead for Planning is responsible for approving and reviewing any changes in respect of Planning Services only).
- Data Protection documentation(ROPAS/Privacy Notices/Retention and Disposal Schedules) shall be reviewed annually by the GDPR Lead or Head of Service and in consultation with the Data Protection Officer to minimise the risk of problems and adverse impact on services.
- Each time a document such as a ROPA/Privacy Notices/Retention and Disposal Schedule is reviewed and changes made, this must be documented by a version control for each document. This must state:
    - The date the document is reviewed
    - the version number
    - the notes/reasons for the changes and
    - the name of the person who has reviewed the document.

18. 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,	SIGO

		CEO and Senior Managers added. Members' responsibilities updated - requirement to register with the ICO removed. Complaints procedure added. Version Control table added.	
3.0	13/05/2020	Agreed by JONG. Finalised for publishing.	SIGO
3.0	28/04/2021	Policy reviewed. Refs to 'GDPR' replaced with 'UK GDPR'. Ref to 'Information Officers' replaced with 'Request for Information Officers' as per formal title.	SIGO

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 ICO and where the breach is likely to result in a risk to people's rights and freedoms.