ADUR & WORTHING
COUNCILS

Information Security Policy Suite

Data Protection Policy

1. Purpose

The purpose of this policy is to ensure appropriate measures are applied to comply with the Data Protection Legislation as at 25th May 2018, namely, EU General Data Protection Regulations (GDPR) and UK Data Protection Bill 2017 (DPA) . At the time of writing the DPA is progressing through Parliament as the Data Protection Bill.

2. Scope

The Councils are committed to the compliance with all Data Protection legislation in respect of personal data and the protection of the “rights and freedoms” of individuals whose information the Council collects and processes.

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

This policy applies to all personal data held, created, modified or accessed from the effective date of this policy. It includes information in any form, no matter whether it is stationary (e.g. an electronic or paper document) or in transit (e.g. file transfer, e-mail, fax, phone, post, courier). It also covers the buildings, premises and systems which contain that information refer to the Buildings, Infrastructure and Equipment Security Policy (ISPS-004).

3. Policy Statement

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

a. ensuring that we comply with the data protection principles
b. meeting our legal obligations as laid down by the Data Protection law
c. ensuring that data is collected and used fairly and lawfully
d. processing personal data only in order to meet our operational needs or fulfil legal requirements
e. taking steps to ensure that personal data is up to date and accurate
f. establishing appropriate retention periods for personal data
g. ensuring that data subjects' rights can be appropriately exercised
h. providing adequate security measures to protect personal data
i. ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
j. ensuring that all staff are made aware of good practice in data protection
k. providing adequate training for all staff responsible for personal data

l. ensuring that everyone handling personal data knows where to find further guidance
m. ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly
n. regularly reviewing data protection procedures and guidelines within the organisation

4 Data Subjects Rights

Data Subjects have the following rights regarding data processing, and the data that is recorded about them:

- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of automated decision-taking process that will significantly affect them
- To not have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller
- To object to any automated profiling that is occurring without consent
- To access the personal data held about them

5. Responsibilities

This section should be read in conjunction with the responsibilities detailed in section 4 of the Information Governance and Security Policy (ISPS-001). 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.

a. to inform and advise the Council and employees about legal obligations to comply with the GDPR and other data protection laws
b. to monitor compliance with the GDPR 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
c. to advise on, and to monitor, data protection impact assessments
d. to cooperate with the Information Commissioner's Office
e. to be the first point of contact for Information Commissioner's Office and for individuals whose data is processed (employees, customers etc).

In addition the Data Protection Officer will be responsible for :

f. Maintain a GDPR Register of Processing activity
g. Ensuring that compliant contracts with Data Processors are in place
h. Manage and report as appropriate any personal data breaches
i. Embed Privacy By Design into service design
j. Annual renewal of notification ICO registration

5.2 Head of Services

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

a. Ensuring that staff are aware of their responsibilities under Data Protection legislation
b. Ensuring employees, including contractors, consultants and volunteers employed to undertake Council business follow the data protection policy and procedures
c. Ensure appropriate resources are in place to enable compliance with the data protection policy
d. Ensure that compliance with data protection legislation under the DPA, GDPR, any other data protection legislation and good practice can be demonstrated

5.3 Staff

All staff :

a. Must be aware of the Data Protection legislations and of their obligations under it
b. Individual staff members may be personally liable for Privacy breaches t if they act outside the authority of the data controller

c. All new members of staff must undertake Data Protection Training and familiarise themselves with the Council's Data Protection Policy and procedures as part of their induction process and in training sessions provided by the Council
d. 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 an information security incident or on a yearly cycle at the Council's discretion
e. Report data privacy breaches to the Data Protection Officer

5.4 Elected Members

All Elected Members:

a. should be made fully aware of this policy and of their duties and responsibilities under the Data Protection legislation
b. handle personal information in their role as politicians or in their role as elected members, they are covered by their party or the Council's notification respectively. As such, they have to handle personal information in line with the requirements of the Council's Data Protection Policy
c. If elected Members use (process) personal information in their constituency work, or are independent elected Members, they must notify with the Information Commissioner's Office as a data controller in their own right

6. Training associated with this Policy

This policy will be included in the Information Security suite of awareness materials and training courses and delivered with reference to the Training Guidelines (ISPS-001b1)

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

7. Monitoring

Compliance monitoring will be carried out by the Council's Information Security Manager (ISM) and through the Council's management structure

7.1 Non-compliance

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

7.2 Review

This Data Protection Policy will initially be reviewed after twelve months and on a three- yearly basis thereafter, refer to the review procedure in Appendix A of the Policy Creation and Style Guidelines (ISPS-001b3)

8. Equality Impact Assessment (EIA)

An equality impact assessment has been completed for the whole Information Security Policy Suite. A copy of the form is available upon request from the Council's Information Security Manager (ISM)

9. Related documents

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

- ISPS-001 Information Governance and Security Policy;
- Other policies in the Information Security Policy Suite;
- Any supporting standards, guidelines and procedures.

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 or data concerning a natural person's sex life or sexual orientation.

Data Subject – any living individual who is the subject of 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 adversely affect the personal data or privacy of the data subject.