Data Protection Policy

October 2023

Data Protection Policy – Contents Page

1. Introduction

1.1 Purpose

Arun District Council (the Council) collects and uses personal data to carry out its business and provide services. This Data Protection Policy sets out how the Council will protect individuals' rights in relation to the access, use, disclosure and storage of their personal data and defines standards to achieve compliance with current legislation.

1.2 Legislation

The UK General Data Protection Regulation (UK GDPR) replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. The UK GDPR sets out both a new legal framework and more specific requirements regarding the processing of personal data about the Council's residents (and all those whose personal data is processed by the Council). Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and wherever possible, that it is processed with their consent.

1.3 Regulation

The Information Commissioner's Office (ICO) is responsible for regulating and enforcing the Data Protection Act 2018 and the UK GDPR.

2. Scope of UK GDPR

2.1 Article 2: Material scope

This Regulation applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by means of personal data (i.e. paper or electronic records) that form part of a filing system or are intended to form part of a filing system.

2.2 Article 3: Territorial scope

This Regulation applies to the Council, being a data controller in the UK, regardless of whether the processing takes place in the UK or not.

3. Definitions

The following definitions shall apply as defined by the Act and the UK GDPR:

Term	Definition
Data	Information which: a) is being processed by means of equipment operating automatically in response to instructions given for that purpose. b) is recorded with the intention that it should be processed by means of such equipment. c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, i.e., a structured set of data accessible according to specific criteria whether centralised, decentralised, or dispersed on a functional or geographical basis. d) does not fall within the above but forms part of an accessible record, i.e., a housing record or e) is recorded information held by a public authority and does not fall within any of the above paragraphs.
Personal Data	Information relating to an identified or identifiable natural person ('data subject'). Personal identifiers can include a name, identification number, location data, 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 Category Data (defined under the UK GDPR)	Personal Data, likely to be more sensitive, about an individual's • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data • health • sex life • sexual orientation
Processing	Any operation or set of operations performed on personal data or 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 Subject	Any living individual who is the subject of the personal data.
Data Controller	The natural or legal person, public authority, agency, or other body which, alone of jointly with others, determines the purpose 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. Where the Council is a Data Controller its Data Processors will be third party contractors acting pursuant to a written contract which must include reference to a range of statutory requirements. Where a third party is the Data Controller, the Council can be a Data Processor where it is acting for and on behalf of the third party in respect of the processing.
Data Asset Owner	At the Council, these are Group Heads of Service. Data Asset Owners must understand what information is held within their Service, what is added/removed, how information is moved and who has access and why. The DAO is not necessarily the creator

	or primary user of the asset, but they must understand its value to the Council.
Consent	Of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Third Party	A natural or legal person, public authority, agency, or body other than the Data Subject, Controller, Processor, and persons who, under the direct authority of the Controller or Processor, are authorised to process personal data.

4. Data Protection Principles

The Council shall adhere to the principles of the UK GDPR which require that personal data shall be:

4.1 processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

4.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

4.7 the Data Controller shall be responsible for and be able to demonstrate compliance with all the above.

5. Responsibilities

The Council shall ensure that:

5.1 It is a registered Data Controller. The registration number for the Council is Z5626915.

5.2 It has specialist staff with specific responsibility for ensuring compliance with the Act and the UK GDPR.

5.3 Individuals processing personal data understand that they are responsible for complying with the data protection principles.

5.4 Individuals processing personal data are appropriately trained to do so.

5.5 Individuals are provided with appropriate data protection support and guidance.

6. Roles

The following roles have responsibility for Data Protection within the Council:

Role	Responsibilities
Data Protection Officer (DPO)	1. Providing data protection support and guidance to the Council to ensure that staff and Councillors are aware of their responsibilities and obligations. 2. Developing and monitoring the biennial mandatory data protection training programme for staff. 3. Providing appropriate training and briefings to Councillors on data protection policies and procedures. 4. Acting as a contact point for data subjects and the Council to ensure that any queries about data protection are dealt with effectively. 5. Monitoring compliance across the Council's functions to ensure that there is consistency and application of data protection rules and procedures. 6. Developing and regularly reviewing the Council's data protection policies and procedures. 7. Developing and regularly reviewing a data retention schedule across the Council working to the Data Retention & Destruction Policy. 8. Facilitating information sharing between the Council and other organisations by developing information sharing agreements where required.
Senior Information Risk Owner (SIRO)	1. Leading and fostering a culture that values, protects, and uses information for the benefit of the Council and its customers. 2. Owning the Council's overall information risk management policies and procedures and ensuring they are implemented consistently across the organisation. 3. Monitoring compliance through the annual assurance statement.
Group Heads	1. Ensuring that the requirements for data protection are integrated into service procedures. 2. Ensuring that staff comply with all relevant policies and procedures within their area of responsibility.
All Council staff	1. Processing information in line with the Act and the UK GDPR. 2. Complying with all policy, procedural and legislative requirements. 3. Undertaking mandatory biennial data protection training.

6.1. The role of Data Protection Officer and Senior Information Risk Owner will be held by the relevant Group Head or Senior Manager and this responsibility confirmed within the Council's Constitution, under Part 7 Section 2.

6.2. The Council shall also establish a corporate officer working group (Information Security Group) to oversee the management of data protection and information risk across the Council comprising the:

Senior Information Risk Owner
Data Protection Officer
Group Head of Organisational Excellence
Head of Technology and Digital

ICT and Digital Manager
Information Governance Manager

6.3 Data Asset Owners must liaise with the Data Protection Officer every 12 months via the Senior Management Team to determine whether any changes need to be made to any owned registers/documents.

7. Privacy Notices

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

7.1.1. what information is being collected.
7.1.2. why the Council collects information.
7.1.3. who the Council may share this information with.
7.1.4. what the Council will do with the information.
7.1.5. how long the Council will keep the information; and
7.1.6. what rights individuals have.

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

A separate privacy notice is available for Councillors.

7.3. Data Asset Owners must liaise with the Data Protection Officer every 24 months via the Senior Management Team to determine whether any changes need to be made to any departmental privacy notices.

8. Individuals Rights

8.1. Individuals have the right to find out what information the Council holds about them through a data subject access request. Requests can be made here.

8.2. The UK GDPR also provides for individuals to have:

8.2.1. the right to be informed about the collection and use of their personal data.
8.2.2. the right of access to their personal data and supplementary information.
8.2.3. the right to have inaccurate personal data rectified or completed if it is incomplete.
8.2.4. the right to have personal data erased in certain circumstances.
8.2.5. the right to request the restriction or suppression of their personal data in certain circumstances.
8.2.6. the right to data portability which allows them to obtain and reuse their personal data for their own purposes across different services.

8.2.7. the right to object to processing in certain circumstances; and
8.2.8. rights in relation to automated decision making and profiling.

8.3. Any complaints made about how the Council processes personal data will be considered by the Data Protection Officer.

9. Data Protection Impact Assessments

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

9.2. The Council will conduct a DPIA for major projects and all contracts which require the processing of personal data or where processing is likely to result in a high risk to individuals' interests. This will be completed by the relevant service and overseen by the Group Head.

9.3. The outcome of a DPIA will be used to influence the design of the project and contract terms and conditions.

10. Data Security and Breach Management

10.1. The Council will ensure that it processes personal data securely by means of appropriate technical and organisational measures. These measures will include adherence to relevant Council policies.

10.2. Access to personal data shall be strictly controlled.

10.3. The Council will investigate all suspected breaches which involve personal data. Where a relevant breach is identified, this will be reported to the Information Commissioner's Office based on UK GDPR requirements. All breaches (or suspected breaches) should be notified by completing the online form via Sharepoint. Advice can be sought at data.protection@arun.gov.uk.

11. Information and Communication Technology

11.1. To understand how to protect our information and ICT systems staff must read the information security policy and ICT acceptable usage agreement.

11.2. When procuring new ICT systems this must be discussed with the Head of Technology & Digital who may ask for a security questionnaire to be completed.

11.3. Any data being processed or stored by an ICT system must be located in the UK

11.4. Any installed programs or apps must comply with the Information Security Policy.

12. Training and Awareness

12.1. A mandatory training programme on data protection, information governance and cyber security is in place for all staff. This training should be re-completed at a minimum of 24-month intervals.

12.2. On joining the Council all new staff are required to undergo an induction programme which includes the above training. In addition, Group Heads are required to ensure that all new staff are aware of the contents of the service specific privacy notices. Amendments to service specific privacy notices will be notified to all relevant staff by the Group Head.

12.3. Appropriate training and briefings on data protection policies and procedures shall be provided to Councillors at a minimum of 24-month intervals, as agreed by the Data Protection Officer in consultation with the Standards Committee.

12.4. All staff and councillors shall be required to sign up to the Council's Information Security Policy at the start of their employment/term of office.

12.5. The Data Protection Officer shall identify appropriate data protection training for any Contractors working within the Council's buildings and such training will then be made mandatory as part of the contract terms and conditions.

13. Information Sharing

13.1. The Council shall ensure that personal data is shared only when it is permitted to do so within the law or where this can be justified.

13.2. Where personal data is shared with an external partner organisation, the Council shall establish formal information sharing agreements to ensure that adequate technical and organisation measures are put in place to protect the personal data.

13.3. Any transfer of personal data between the Council and partner organisations shall be carried out using a secure method agreed between the Council and the partner organisation.

13.4. Where personal data needs to be shared within the Council under a lawful or justified purpose, the Council shall ensure that access rights are approved by the relevant Group Head or their representative and the individual has been made aware of the intention to share information through a privacy notice.

14. Contracts

14.1. All Council contracts shall include appropriate terms to ensure that personal data is handled in accordance with the Act and the UK GDPR. This will involve conducting a DPIA before quotations are sought or a contract is tendered.

14.2. 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 unless required by legislation.

14.3. The Council 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, including appropriate contractual terms.

15. Relevant Council Policies

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

Information Security Policy
Privacy Policy
Homeworking Policy
Records Retention and Disposal Policy
Data Subject Access Request Policy

Equality and Diversity

Equality and Diversity is important to the Council, and we are committed to making sure that people are treated fairly and with dignity. This means that we sometimes have to ask for or hold special category data in order to design and provide equality compliant services. Our aim is to remove unnecessary barriers for everyone who works for us or uses our services. All staff receive equality and diversity training as part of their role.

Policy Review

This policy was adopted by the Corporate Support Committee and will be reviewed every 3 years by the Data Protection Officer. The next review will be due October 2026.