ARUN DISTRICT COUNCIL

Data Protection Policy

Document Control

Document Owner	Liz Futcher, Data Protection Officer
Version	V2
Date	25 September 2018

Version History

Date	Version Number	Revision Notes	Author
020518	V1	Approved by Full Council	Liz Futcher
250918	V2	Updated by Group Head under delegated authority to reflect requirements of Data Protection Act 2018	Liz Futcher

1. Introduction

1.1. The Data Protection Act 2018 (the Act) and the General Data Protection Regulation (GDPR) aim to protect all personal data which is collected, processed, stored and disposed of by an organisation.

1.2. Arun District Council (the Council) has a statutory duty to comply with the requirements of both the Act and the GDPR as it collects personal data when conducting its business.

1.3. The Information Commissioner's Office (ICO) is responsible for regulating and enforcing the Act and the GDPR.

2. Aim

2.1. The aim of this policy is to demonstrate the Council's compliance with the principles of the Act and the GDPR.

2.2. The policy also aims to demonstrate that the Council understands its responsibilities for promoting accountability and good governance, and has put appropriate technical and organisational measures in place to minimise the risk of data breaches.

3. Scope

3.1. The policy applies to:

3.1.1. All personal data processed by the Council regardless of format.
3.1.2. Any individual processing of personal data held by the Council.

4. Definition of Terms

4.1. The following definitions shall apply as defined by the Act and the 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 highly structured readily accessible paper filing system; 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 identifiable person who can be directly or indirectly identified in particular by reference to an identifier. Personal identifiers can include a name, identification number, location data or online identifier.
Special Category Data (defined under the GDPR)	Sensitive information about an individual's • race • ethnic origin • politics • religion • trade union membership • genetics • biometrics (where used for ID purposes) • health • sex life • sexual orientation
Processing	Obtaining, recording or holding the information or data, or carrying out an operation or set of operations on the information or data.
Data subject	An individual who is the subject of the personal data
Data Controller	A person who alone, jointly or in common with other persons, determines the purposes and means of processing personal data. A data controller may also act jointly with another organisation to process personal data. The controller must ensure contracts with any processors comply with GDPR obligations.
Data Processor	Any person, other than an employee of the data controller, who is responsible for processing personal data on behalf of the data controller. The processor will have a legal liability if they are responsible for a breach.

5. Data Protection Principles

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

5.1.1. processed lawfully, fairly and in a transparent manner in relation to individuals;

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

5.1.3. adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;

5.1.4. accurate and, where necessary, kept up to date;

5.1.5. 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; and

5.1.6. 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.

5.2. The Council shall also be responsible for, and be able to demonstrate, compliance with these principles.

6. Responsibilities

6.1. The Council shall ensure that:

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

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

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

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

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

7. Roles

7.1. The following roles shall be established:

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 annual 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.
Council staff	1. Processing information in line with the Act and the GDPR. 2. Complying with all policy and procedural requirements. 3. Undertaking mandatory annual data protection training.

7.2. The role of Data Protection Officer and Senior Information and Risk Owner will be held by the relevant Group Head and this responsibility confirmed within the Scheme of the Delegation, at Part 4 of the Council's Constitution.

7.3. The Council shall also establish a corporate officer working group to oversee the management of data protection and information risk across the Council comprising the:

7.3.1. Group Head of Corporate Support (SIRO)
7.3.2. Group Head of Council Advice & Monitoring Officer (DPO)
7.3.3. Chief Internal Auditor
7.3.4. ICT and Service Improvement Manager
7.3.5. ICT Technical Manager

8. Privacy Notices

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

8.1.1. what information is being collected;
8.1.2. why the Council collects information;
8.1.3. who the Council may share this information with;
8.1.4. what the Council will do with the information;
8.1.5. how long the Council will keep the information; and
8.1.6. what rights individuals have.

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

9. Individuals Rights

9.1. Individuals have the right to find out what information the Council holds about them through a data subject request. Requests can be made via: https://www.arun.gov.uk/data-protection

9.2. The GDPR also provides for individuals to have:

9.2.1. the right to be informed about the collection and use of their personal data;
9.2.2. the right of access to their personal data and supplementary information;
9.2.3. the right to have inaccurate personal data rectified or completed if it is incomplete;
9.2.4. the right to have personal data erased in certain circumstances;
9.2.5. the right to request the restriction or suppression of their personal data in certain circumstances;
9.2.6. the right to data portability which allows them to obtain and reuse their personal data for their own purposes across different services;
9.2.7. the right to object to processing in certain circumstances; and
9.2.8. rights in relation to automated decision making and profiling.

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

10. Data Protection Impact Assessments

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

10.2. The Council 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.

10.3. DPIAs shall be considered as part of the Arun Improvement Programme process for reviewing the viability and business case for new ICT systems.

11. Data Security and Breach Management

11.1. The Council 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.

11.2. Access to personal data shall be strictly controlled.

11.3. The Council shall investigate all suspected breaches which involve personal data. Where a breach is identified, this will be reported to the Information Commissioner's Office based on GDPR requirements.

12. Training and Awareness

12.1. A mandatory training programme for all staff was undertaken over February to April 2018 covering the requirements of the GDPR and management of cyber security. All Councillors were also briefed on the changes affecting their role in March and April 2018.

12.2. On joining the Council all new staff shall be required to undergo an induction programme including data protection and cyber security training.

12.3. The Data Protection Officer shall agree an ongoing annual programme of mandatory data protection training for all the Council's staff with the Corporate Management Team to be run from 2019 onwards.

12.4. Appropriate training and briefings on data protection policies and procedures shall be provided to Councillors on a biannual basis as a minimum, as agreed by the Data Protection Officer in consultation with the Cabinet Member for Corporate Governance.

12.5. 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.

12.6. The Data Protection Officer shall identify appropriate data protection training for any Contractors working within the Council's buildings.

13. Information Sharing

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

13.2. Where personal information 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 information.

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

13.4. Where personal information 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 is informed 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 GDPR.

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.

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.

15. Policy Review

15.1. This policy will be reviewed on an annual basis by the Data Protection Officer.

16. Relevant Council Policies

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

16.1.1. Information Security Policy
16.1.2. Privacy Policy
16.1.3. Homeworking Policies
16.1.4. Clear Desk/Clear Screen Policy
16.1.5. Documentation Retention & Disposal Policy
16.1.6. Human Resources Data Protection Policy