Data Protection Policy

Author	Version	Date	Amendments
Caroline Pegg	**1**	31/01/2018	N/A
Caroline Pegg	**2**	15/10/2018	Addition of Clause 1.9 – appropriate policy document
Caroline Pegg	**3**	23/03/2021	Minor changes

CONTENTS

1. POLICY STATEMENT

1.1. This document sets out West Sussex County Council's Data Protection Policy and how it complies with the Council's duties under the Data Protection Act 2018 and the General Data Protection Regulations (the Act).

1.2. The Act regulates the way in which personal information about individuals, whether held on computer or in a manual filing system, is obtained, stored, used, disclosed and destroyed.

1.3. The Council needs to obtain and use personal data and sometimes special category data (sensitive personal data) about people with whom it deals in order to perform its functions and to comply with its statutory duties. This includes information on current, past and prospective service users, employees, suppliers, clients, customers, and others with whom it communicates. It may include all persons who live, work, visit or who receive education within the County and many others who do not.

1.4. The Council regards the lawful and correct treatment of personal information as critical to the success and effectiveness of its operations, and to maintaining the confidence of those it serves. It is essential that it respects the rights of all persons whose personal information it holds, that it treats personal information lawfully and correctly in accordance with the Act and that it is able to show that this is the case.

1.5. Failure to comply with the Act infringes the rights of individuals and may place them at risk of loss or harm. It also exposes the Council to challenge, to legal claims and to substantial financial penalty.

1.6. This Policy applies to all staff and elected members and the Council expects all of its staff and elected members to comply fully with this Policy and the Principles of the Data Protection legislation (set out in section 2 below). Disciplinary action may be taken against any employee who breaches any of the instructions or requirements forming part of this policy. Elected Members should adhere to this policy so as to ensure compliance with the Member Code of Conduct and the Council's obligations in relation to confidentiality.

1.7. Third parties such as partners, public and private organisations or contractors with whom the Council shares personal data or who hold data on the Council's behalf will be expected to enter into and adhere to formal agreements or contractual obligations with the Council incorporating the principles of this policy and the requirements of the Act. Such agreements or contracts must define the purposes for which personal data is supplied to or held by the other party and require contractors to have in place appropriate organisational and technical measures to protect the data and processes to enable the exercise of the rights of individuals.

1.8. Details of the Council's purposes for holding and processing data can be viewed on the data protection register. The Council's registration number is Z6413427. This registration is renewed annually and updated as and when necessary.

1.9. This policy shall be regarded as the 'appropriate policy document' where The Council processes data under a condition in;

- Paragraph 1 of Schedule 1 DPA 2018 (Employment, Social Security or Social Protection)
- Part 2 Schedule 1 DPA 2018 (Substantial Public Interest paragraphs 6-28)
- Part 3 Schedule 1 DPA 2018 (Criminal convictions as an enforcement authority)

2. THE DATA PROTECTION PRINCIPLES

2.1 Personal data must be:

(1) processed lawfully, fairly and in a transparent manner;

(2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(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;

(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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(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.

2.2 Processing Special Category and Criminal Data

Special category data and Criminal Data shall only be processed lawfully if it is carried out in accordance with this policy and the data protection principles at 2.1.

2.2.1 Accountability Principle

The Council shall be responsible for and be able to demonstrate compliance with these principles where it processes Special Category and/or Criminal data.

The Council shall ensure, where special category or criminal data is processed, that;

- It carries out a DPIA for any high-risk personal data processing which includes special category and criminal data. Further information can be found in the Data Protection Impact Assessment Policy.
- There is a record of that processing, and that the record will set out, where possible, the envisaged time limits for retention of the different categories of data.

3. GIVING EFFECT TO THE POLICY – RESPONSIBILITIES OF OFFICERS

3.1 The Council is a Data Controller under the Act and must comply with the Data Protection Principles and be able to demonstrate compliance.

3.2 The Chief Executive shall be accountable for the implementation and effectiveness of this policy

3.3 Where an Elected Member has access to and processes personal information on behalf of the Council the Member does so under the Council's registration and must comply with this policy. When Members process personal data whilst acting as a representative of residents of their electoral division and /or whilst representing a political party, they do so as Data Controllers registered separately with the Information Commissioner's Office.

3.4 All Executive Directors and Directors are responsible for implementing safe and sound data protection procedures within their services and the operation of those services and ensuring the proper security of information held. Directors should have regard to this Policy, the Information Sharing Policy and the Acceptable Use Policy when formulating any policies or procedures which make use of personal data.

3.5 The Council's Constitution, through its scheme of delegation, will ensure that a named individual has specific operational responsibility for data protection matters corporately. That person is The Data Protection Officer. The Data Protection Officer shall report to the Chief Executive.

3.6 Within the Directorate of Law and Assurance there will be a Data Protection Team with specific responsibility for data protection compliance and for advising and training on data protection matters.

The Data Protection Team Manager shall report to the Data Protection Officer.

3.7 Within the Data Team two Data Management and Access Officer (adults and children) will be responsible for taking the lead on data protection matters and request handling.

3.8 The Council shall have in place an Information Governance Group to oversee the effective operation of the Council's data protection arrangements and which is led by and whose operation is the responsibility of the Data Protection Officer.

3.9 It is the responsibility of all staff to ensure that their working practices comply with the Data Protection principles and that information held by the Council is accurate and up-to-date.

3.10 All new staff will receive basic training on the Act as part of their induction. Managers should ensure all staff for whom the manager is responsible receive appropriate training on the Data Protection legislation, on the application of this Policy and on their individual responsibilities.

4. SECURITY OF DATA

4.1 All staff are responsible for ensuring that personal data which they use or process is kept securely and is not disclosed to any unauthorised person or organisation. Access to personal data should only be given to those who have and can show a need for access to the data for the purpose of their duties.

4.2 The Data Protection Officer shall ensure that an Acceptable IT Use Policy (AUP) is in place that covers all aspects of activity and conduct to ensure compliance with the Council's obligations in relation to electronically held information and that such a Policy is kept up to date and drawn to the attention of all staff. All staff and elected members must read and comply with the AUP, which must be signed as read by all staff before access to information containing personal data is permitted. The AUP is permanently accessible on the desktop of every member of staff's laptop/PC.

4.3 Personal data should not be left where it can be accessed by persons not unauthorised to see it or have access to it by reference to this Policy and the Data Protection Principles.

4.4 Procedures shall be put in place by the Director responsible for Council buildings and facilities in accordance with the Council's scheme of delegation, relating to access to the Council's buildings so as to ensure the security of data and compliance with this policy and any requirements relating to controlling access to buildings and particular parts of buildings should be communicated to all staff and members and adhered to by all.

4.5 Personal data which is no longer required must be destroyed appropriately, for example, by shredding or, in the case of computer records, secure deletion. Computers must have all personal information securely deleted using the appropriate software tools when they are disposed of in accordance with the Council's policy for IT Asset Management. Personal data must be destroyed in accordance with the Council's retention schedule.

4.6 Staff and elected members who work from home must have particular regard to the need to ensure compliance with this policy and the policy for Working outside WSCC Offices and the Acceptable IT use Policy. The security and proper processing of data outside offices and usual places of work and whilst travelling must be ensured.

4.7 Personal data security breaches will be detected, reported and investigated in accordance with the data breach security management process. Serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office by the Data Protection Officer.

4.8 All staff will be aware of and follow the data breach security management process accessible on the WSCC intranet and included in induction training for all new members of staff.

5. DATA SUBJECTS' RIGHTS

5.1 Members, staff and members of the public have the following rights in relation to their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with
- to access their data
- to rectification of the record
- to erasure of their data

- to restrict processing
- to data portability
- to object to processing
- not to be subject to automated decision-making including profiling.

5.2 The Data Protection Officer will ensure appropriate processes are in place for the exercise of any of these rights.

5.3 Requests for access to personal data (Subject Access Requests) are processed via the Data Management and Access Officers in the Data Protection Team.

5.4 The Council aims to respond promptly to a subject access request and in any event within the statutory time limit. Subject access requests will be managed and tracked using an electronic system.

6. DISCLOSURES TO THIRD PARTIES

6.1 All staff and Elected Members have a responsibility to ensure that any personal data they see or hear is not disclosed to third parties unless there is clear and specific authority to do so. This includes personal data and information extracted from such data, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or by allowing it to be read on a computer screen.

6.2 The Council will only share personal data with other organisations and third parties where the sharing is necessary to achieve a clear objective and it is fair and lawful to do so. Routine sharing of data between organisations for an agreed lawful purpose will be undertaken in accordance with the Information Sharing Policy.

6.3 Disclosure within the Council either to staff or elected members will be on a need to know basis or to enable the most effective discharge of their responsibilities and in compliance with the Act. Such disclosure of data may only take place if a lawful basis is identified and in accordance with the Data Protection Principles.

7. ENSURING COMPLIANCE

The Council will ensure that:

7.1 Each Directorate documents what personal data is held by the services of that Directorate, where it came from, who it is shared with and that the specification of data management systems operated by the Directorate enables compliance with the Act.

7.2 Privacy Notices which explain to individual persons the data held by the Council relevant to them will contain the following information:

- The name and contact details of the Data Controller and Data Protection Officer
- The purpose and legal basis of processing the data.
- Retentions period for the date
- The identity of those with whom the data is shared.
- The rights to request rectification, to request erasure, to withdraw consent, to complain, to know about any automated decision making and the right to data portability where applicable.

7.3 Where processing is reliant on consent from the individual whose data is held the Council will ensure consent is obtained and is current and actively managed. Consents will contain a positive opt-in with a mechanism for easy withdrawal of consent.

7.4 Legal advice, training and guidance are available to all staff and elected members. Core guidance, practice, procedures and policies shall be held on the County Council's intranet. The Data Protection Officer shall ensure that training resources are up to date and that Directorates promote and ensure the take up of training and advice by staff.

7.5 The development and promulgation of best practice and co-ordination of data protection policies and procedures in the Council will be the responsibility of the Data Protection Officer, supported by the Information Governance Group which will include representatives from all Directorates.

7.6 It is the responsibility of all staff considering proposals for the creation of any new databases or significant changes to current databases containing personal data to carry out a privacy impact assessment at an early stage in the development of such proposal.

7.7 The Council will have in place a compliance programme to monitor data processing. The status of compliance activities should be monitored by the Council's Information Governance Group or a delegated DPA sub-group.

This policy was approved by Tony Kershaw Director of Law and Assurance on 25th January 2018 acting as the Council's Data Protection Officer.

Reviewed 26th July 2018

Reviewed 23rd March 2021

It will be reviewed by the DPO no later than 25th January 2023

Appendix 1 Definition of Terms

To aid the understanding of this document and the provisions of the Data Protection Act the following definitions are provided for assistance:

Data is any information held or recorded in any form by a public authority.

Automated decision-making means a decision made without human intervention solely by automatic means.

Data Controller means the Council as the organisation who determines how data is processed.

Data Processor means any person, other than an employee of the Council, who processes data on behalf of the data controller e.g. someone contracted to the Council to print documents containing personal data.

Data subject is the individual about whom personal data is processed.

Personal Data means Data which relates to a living individual who can be identified-

(a) either directly from that data, or
(b) indirectly from that data and other information, which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy Notice means a notice created by the data controller and made available to the data subject which explains how personal data is being processed.

Special category data (Sensitive Personal Data) means personal data consisting of information as to any of the following:

- racial or ethnic origin
- political opinion
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- genetics;
- biometrics (where used for ID purposes);
- physical or mental health or condition
- sexual life or sexual orientation.
- personal data relating to criminal allegations, proceedings or convictions.

Criminal data – includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

Processing means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including organisation, adaptation or alteration, disclosure and destruction of the information or data and includes onward disclosure or sharing.

Profiling means the creation, manipulation collation or bringing together of information held or acquired about an individual for the purpose of recording or predicting an individual's conduct or behaviour.