South Derbyshire District Council

Data Protection Policy

Version Control

Version	Reason for review (review date/legislation/process chances)	Author (A) / Reviewer (R)	Effective date
1.0	Review and update following Audit of Procedures	Kevin Stackhouse	01/04/14
2.0	Update ahead of GDPR	Kevin Stackhouse	01/02/18
2.1	Policy Review	Kevin Stackhouse	01/02/19
2.2.	Policy Review	Anthony Baxter	01/06/22
2.3	Policy Review	Anthony Baxter	29/01/25
2.4	Policy Review and Update following The Data Use and Access Act 2025 (DUAA)	Jemma Handley	30/04/26

Approvals

Approved by (Committee/Leadership Team)	Date
Kevin Stackhouse	01/02/2018
Leadership Team	11/05/2022
Leadership Team	29/01/2025
Finance and Management Committee	30/04/2026

Data Protection Officer

Date: April 2026

Contents

1.0 Introduction

1.1 In carrying out its work South Derbyshire District Council processes the personal data of living individuals such as its staff, customers, service users and contractors. This processing is regulated by the UK GDPR and Data Protection Act 2018 (as amended).

1.2 It is the duty of the Council as a data controller to comply with the data protection principles (see section 4 of this policy) with respect to personal data. This policy describes how the Council will discharge its duties in order to ensure continuing compliance with the UK GDPR in general and the data protection principles and rights of data subjects in particular.

2.0 Purpose

2.1 This policy forms part of South Derbyshire District Council's commitment to the safeguarding of personal data processed by its staff and demonstrating its accountability with statutory obligations under Data Protection Legislation. Processing has a very broad definition, and includes activities such as accessing, collecting, creating, storing, consulting, amending, disclosing and destroying data. The Council is a data controller for most of the personal data it processes. This policy explains how the Council will meet its data protection obligations and protect individuals' information rights.

3.0 What is our policy?

3.1The key objectives of this Policy are to:

- handle personal data lawfully, fairly and transparently
- protect personal data through appropriate security and governance
- uphold individuals' data protection rights
- demonstrate compliance and accountability

3.2 All colleagues of the Council are accountable for compliance with this Policy and the referenced legislation.

4.0 Definitions

4.1 Listed in Appendix B.

5.0 Roles and Responsibilities

5.1 Roles

The Council has governance arrangements to support compliance, including:

- A Senior Information Risk Owner (SIRO) for strategic oversight of information risk
- A Data Protection Officer (DPO) who provides independent advice and monitoring
- A designated Information Asset Owner (IAO) responsible for compliance with data protection and data security for their service. Unless stated otherwise, the IAO will be each Head of Service.

5.2 Responsibilities

- All Council employees, officers and agents must:
- Fully understand their data protection obligations
- Not store data incorrectly, be careless with it or otherwise cause the Council to breach data protection laws and its policies
- Process personal data in accordance with the data protection principles
- Check that any data processing activities they are dealing with comply with our policy and are justified, necessary and proportionate.
- Only access personal data where it is necessary for their role
- Ensure personal data is accurate, kept up to date and only retained for as long as necessary
- Follow all relevant policies, procedures and guidance relating to information governance
- Complete mandatory annual data protection and cyber security training
- Not use data in any unlawful way
- Report actual or suspected personal data breaches immediately in line with the Council's breach reporting procedure
- Ensure appropriate security measures are in place when handling personal data (including clear desk, lock screens, secure disposal, and appropriate use of ICT systems)
- Not disclose personal data to unauthorised individuals or organisations
- Comply with this Policy at all times
- Ensure that all colleagues are fully aware of the content of this policy and handle personal data in line with this policy.

5.3 Managers are responsible for:

- Ensuring that this Policy is communicated to all employees including temporary staff and that it is adhered to. It must be communicated to all elected members, contractors, agents and partners working for or on behalf of the Council.
- Ensuring all employees complete the mandatory DPA training and keep abreast of any developments relating to their area.
- Raise concerns, notify the Data Protection Officer of breaches or errors, and report anything suspicious or contrary to this policy or the Council's legal obligations.

5.4 Authorised users:

- All authorised users must ensure that any request for information they receive is dealt with in line with Data Protection Legislation and this Policy.
- All elected members, contractors, agents and partners working for or on behalf of the Council must complete the mandatory data protection training.

6.0 Legislation, guidance and standards

- 6.1 The Council complies with applicable data protection and related legislation including:UK GDPR
- Data Protection Act 2018 (as amended)
- The Human Rights Act 1998
- Privacy and Electronic Communications Regulations 2000 (as amended)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004

7.0 The data protection principles relating to the processing of personal data

7.1 The Council shall comply with the principles defined in Data Protection Legislation. All colleagues must comply with these principles at all times as they form the basis upon which Data Protection Legislation is built.

7.2 The Principles defined in Article 5(1) & (2) of the UK GDPR says that:

7.2.1 **Principle 1 - Lawful, fair and transparent** – Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the individual. This means the Council must:

- Identify and document an appropriate lawful basis for all processing of personal data
- Ensure processing is fair, proportionate and not carried out in a way that is unjustified, misleading or unexpected
- Be open and clear with individuals about how their personal data is used
- The Council will meet its transparency obligations by providing clear and accessible privacy information, including through Privacy Notices, so that individuals understand how and why their personal data is processed.

7.2.2 **Principle 2 - Limited for its purpose** - Data can only be collected for specified, explicit and legitimate purposes. This means that a clear purpose is needed from the outset on collection of personal data and what the purpose of processing is. As a general rule, if the new purpose is either very different from the original purpose, if it is unexpected, or would have an unjustified impact on the data subjects then it is likely to be incompatible with the original purpose.

7.2.3 **Principle 3 - Adequate, relevant and not excessive** - The Council must do everything it can to collect only the data required to fulfil our purpose for collecting it and that clear documentation is available which explains why each category of personal data is needed. This is particularly important for special category data or

criminal data as excessive retention of health or criminal conviction data can have a huge impact on data subjects if used inappropriately.

7.2.4 **Principle 4 - Accurate** - All Council colleagues are required to take reasonable steps to verify the records held are accurate. Where data is inaccurate or misleading in any way it will be crucial that issues are investigated and correct information should be found, confirmed as accurate and recorded appropriately to correct the error.

7.2.5 **Principle 5 - Data Retention** - The Principle of "storage limitation" otherwise known as retention defines that data cannot be stored longer than necessary for the purpose in which it is held. The effective and timely deletion/destruction of personal data which is no longer needed reduces the risk of it being used in error.

7.2.6 **Principle 6 - Security** - Personal Data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage. This principle underpins the Council 's broader information security responsibilities and applies to all forms of information, whether physical or electronic. The Council uses appropriate technical and organisational measures to protect personal data against unauthorised access, loss or misuse, in line with its information security arrangements.

7.2.7 **Principle 7 – Accountability** – The Council will demonstrate its compliance with all data protection principles when processing personal data.

8.0 The Duty of Confidentiality

8.1 The Council is subject to a common law duty of confidence in respect of information obtained in confidence. Information is considered confidential where:

- it has the necessary quality of confidence (i.e. it is not otherwise publicly available); and
- it has been provided in circumstances giving rise to an obligation of confidence

8.2 Confidential information must not be disclosed without lawful authority. Such authority may arise where:

- Consent has been obtained by the information provider; or
- The disclosure is necessary to safeguard the individual, other individuals, or where disclosure is in the public interest; or

- The Council has a legal duty to disclose the information for example, to comply with a court order.

8.3 Any justification for setting aside an individual's right to confidentiality must be substantial and overarching; for example 'public interest' tests require specialist knowledge and training of colleagues to determine this reason.

9.0 Personal Data

9.1 Personal Data is any information relating to an identified or identifiable natural person (the "Data Subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier. Personal Data includes (but is not limited to):

- name
- address
- date of birth
- email address
- telephone number
- national insurance number
- employee or customer reference numbers
- online identifiers (such as IP addresses)
- location data

9.2 Personal Data may also include information which, when combined with other data held by the Council, can identify an individual.

9.3 Under the Data Protection Legislation and the Information Commissioner's Office guidance, the Council must ensure that all Personal Data is processed in accordance with the Data Protection Principles listed at Section 7 above. Processing must be necessary for a specified purpose and supported by an appropriate lawful basis under Article 6 of the UK GDPR.

9.4 Where Personal Data is processed, services must ensure that individuals are informed through clear and accessible privacy notices, and that appropriate technical and organisational measures are in place to protect the data.

9.5 Special Categories of Data

9.6 Special categories of data create more significant risks to a person's fundamental rights and freedoms and as such the DPA imposing stricter conditions on the processing of such data. Special categories of data include:

- race
- ethnic origin

- politics
- religion
- trade union membership
- genetics
- biometrics
- health
- sexual orientation

9.7 In cases where such data is being processed there is a higher threshold under Data Protection Legislation. There are a separate set of conditions, outlned in Article 9 UK GDPR, one of which must be satisfied before any data above is processed.

9.8 Additionally, some processing of special category data and criminal offence data requires an “appropriate policy document” under Data Protection Legislation.

9.9 Criminal Offence Data

9.10 Under Data Protection Legislation there are specific rules regarding the processing of Personal Data relating to criminal convictions, allegations and offences. Such data shall be carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

9.11 The principles in section 7 of this Policy will also apply to this data.

9.12 When tasked with processing data relating to criminal offences or crime an appropriate statutory rule must be identified permitting use of the data for a valid reason e.g. crime prevention.

10.0 Accountability and transparency

10.1 All employees of the Council must ensure accountability and transparency in all use of Personal Data. The IAO of the Personal Data must show how the Council complies with each Principle. IAOs are responsible for ensuing the Council’s information asset inventory reflects their service’s data processing activities and their service’s compliance with Data Protection Legislation.

10.2 Officers are responsible for understanding their particular responsibilities to ensure the Council remains compliant with data protection legislation.

10.3 Privacy notices and transparency

The Council provides privacy notices explaining how personal data is collected, used, shared, retained and individuals' rights. The Council's privacy information is available at: https://www.southderbyshire.gov.uk/privacy

10.4 Sharing information with third parties

The Council may share Personal Data with third parties where there is a lawful basis to do so and where it is necessary and proportionate for the purpose. This may include sharing information with:

- other public authorities
- partner organisations
- service providers acting on behalf of the Council

The Council will ensure that appropriate safeguards are in place when sharing Personal Data, including contractual arrangements where required.

Personal Data may also be disclosed where required or permitted by law. This includes, for example, disclosures to law enforcement agencies, regulatory bodies, or other organisations for the purposes of preventing or detecting crime, safeguarding individuals, protecting public funds, or complying with legal obligations.

11.0 Data breaches

11.1 A Personal Data breach is when personal information is lost, accessed, disclosed, altered or destroyed without proper authorisation. If a breach occurs, the Council will act promptly to contain and investigate the incident, assess any risks to individuals, and take appropriate steps to mitigate any impact.

11.2 Where required, the Council will report the breach to the Information Commissioner's Office within 72 hours and inform affected individuals if there is a high risk to their rights and freedoms.

12.0 Retention and storage

12.1 Personal Data is retained only for as long as necessary in accordance with the Council's retention schedules and legal obligations. When no longer required, personal data is securely deleted or disposed of in line with the Council's records management procedures.

13.0 Transferring data outside of the UK

13.1 Strict guidelines are in effect for sharing of Personal Data outside the UK. These restrictions apply to all personal data transfers.

13.2 Where personal data is transferred outside the UK, the Council ensures appropriate safeguards are in place in line with the UK GDPR.

14.0 Privacy by Design and Default

14.1 The Council adopts a Privacy by Design and by Default approach. The term “Privacy by Design and Default” means embedding data protection considerations and safeguards into processes, systems and services from the outset, ensuring compliance is built in rather than applied retrospectively.

14.2 The Council implements appropriate information governance and accountability measures to ensure compliance with data protection legislation. This includes undertaking Data Protection Impact Assessments (DPIAs) where required, and establishing appropriate contractual controls, including Data Processing Agreements and Data Sharing Agreements, when engaging third parties or sharing personal data. These measures support the Council’s Privacy by Design and by Default approach and ensure that data protection risks are effectively identified and managed.

15.0 Rights of individuals

15.1 Under the Data Protection Legislation, all individuals (Data Subjects) have rights in respect of the Personal Data held about them. The Council will ensure individuals can exercise these rights and provide services to facilitate such requests. All Colleagues must recognise any of the following as statutory rights under the UK GDPR:

15.2 Individuals have rights in relation to their Personal Data, including:

right to be informed
right of access
right to rectification
right to erasure (in certain circumstances)
right to restrict processing
right to object
rights relating to automated decision-making.

15.3 The Council will respond to requests from individuals in accordance with statutory timescales and will ensure that appropriate processes are in place to recognise and handle such requests.

15.4 In some cases, rights may be subject to exemptions or limitations as set out in legislation. Where this applies, the Council will ensure that any restriction of rights is lawful and proportionate.

15.5 Individuals can find further information about their rights and how to exercise them via the Council's privacy notices or by contacting the Council directly. Individuals also have the right to raise concerns with the Information Commissioner's Office (ICO).

15.6 For more information on how the Council processes individuals' data, there is a detailed Privacy Notice section of the Council's website.

15.7 Where requested, an Internal Review of how the Council processed a Data Subject Right request will be carried out by an officer within 30 working days from receipt.

15.8 Individuals are entitled to submit a request for an Internal Review within three months of receiving the response to their Subject Access Request. The Council will consider whether to respond to requests for an Internal Review outside of these timescales although it is not obliged to do so

16.0 Authorised Users

16.1 Authorised users will only have access to personal information where that access is essential to their duties. Authorised users should discuss with their line manager any instance where access rights require clarification. Access rights are not to be regarded as permanent and are subject to change at any time depending upon the nature of the duties being fulfilled by the authorised user.

16.1 Authorised users with access to personal information must be familiar with the requirements of the DPA and familiar with the content of this Policy.

16.2 Authorised users should only record information about an individual which is relevant, and should be aware that they may be required to justify what has been written and be prepared for that information to be released as part of a subject access request.

16.3 Any authorised user who is found to have inappropriately divulged personal information will be subject to investigation under the Council's disciplinary procedure, which may result in dismissal and possible legal action. Where the authorised user is an elected member they will be subject to investigation under the Code of Conduct set for councillors

16.4 All authorised users must follow good practice as indicated by the DPA and any such codes of practice issued by the Office of the Information Commissioner or the Council, when processing Personal Data.

17.0 Direct Marketing

17.1 The Council may process Personal Data for direct marketing purposes in accordance with data protection legislation and the Privacy and Electronic Communications Regulations (PECR).

17.2 Where Personal Data is used for marketing, the Council will ensure that individuals are provided with clear information about how their data will be used and, where required, obtain valid consent. In other cases, the Council may rely on an appropriate lawful basis, such as legitimate interests, ensuring that the rights and freedoms of individuals are not overridden.

17.3 Individuals have the right to object to direct marketing at any time, and the Council will respect such requests promptly.

18.0 Data Protection Complaints Procedure

18.1 This section sets out the Council ’s procedure for handling data protection complaints in compliance with the UK GDPR, Data Protection Act 2018 and requirements under the Data (Use and Access) Act 2025 (“DUAA”).

18.2 A data protection complaint is any expression of dissatisfaction from an individual about how the Council collects, uses, stores or shares their personal information.

18.3 Individuals may make a complaint by completing the online Data Protection Complaint Form on the Council ’s website, emailing the Data Protection Officer (DPO) at dataprotection@southderbyshire.gov.uk writing to the Council and marking the correspondence for the attention of the DPO

18.4 The Council will acknowledge receipt of a complaint within 30 days, and provide a clear explanation of the next steps.

18.5 The DPO (or a delegated officer) will investigate the complaint and will:

- review the complaint and the information provided
- liaise with relevant services
- assess whether the Council ’s processing has complied with data protection law
- determine whether corrective action is required

18.6 The Council will provide a full response without undue delay, taking into account the complexity of the issues raised. The responses will:

- address each point raised
- explain the outcome of the investigation
- set out any steps the Council has taken or will take
- provide details of how to escalate to the ICO if the individual remains dissatisfied

18.7 If the individual is unhappy with the Council 's final response, they may complain to the ICO: Information Commissioner's Office www.ico.org.uk Telephone: 0303 123 1113

18.8 Data protection complaints follow this dedicated process and will not be handled under the Council 's general complaints policy. Where a complaint spans both data protection and service issues, the DPO will coordinate the appropriate route. Formal complaints outside the scope of data protection will be processed following the corporate complaints procedure.

19.0 Elected Members

19.1 Councillors are involved with Council activities acting in three different roles:

- As member of a Committee. Councillors are appointed to committees as a member of The Council to provide decision making.
- As representative of their Ward, for example, acting on behalf of their Ward to improve services, raise issues and handle complaints related to their locality. Such complaints may relate to a constituent or group of constituents living within their locality.
- As representative of a political party, particularly during elections. However, when acting on behalf of a political party Councillors are entitled to rely upon the party registration rather than The Council which should be considered and clearly defined where responsible for the handling of Personal Data.

19.2 The Council is Data Controller for data processed for the administration of Council business linked to the role listed as above.

19.3 When an elected member's term of office expired or otherwise ceases, they must arrange for the transfer and/or secure disposal of all personal information held by them or their support staff in relation to their role as member of the Council and representative of their Ward.

19.4 Where information requires transfer to Council systems, the Head of Legal and Democratic Services, or their representative, in consultation with the Data Protection Officer will make the necessary arrangements for the transfer and future management of the information transferred.

20.0 Compliance with the Data Protection Policy

20.1 The Data Protection Officer monitors compliance with this Policy and advises on data protection obligations. All officers are responsible for ensuring that Personal Data is processed in accordance with this policy.

20.2 Heads of Service, acting as IAOs, are accountable for compliance within their service areas, including the implementation and maintenance of appropriate documentation and controls.

20.3 All colleagues are required to handle personal data in a manner that ensures its confidentiality, integrity and availability. The Council has appropriate policies, procedures and training in place to support this and to ensure that Personal Data is handled securely and in accordance with data protection legislation.

20.4 The processing of Personal Data by Councillors must at all times be in accordance with the standards and Code of Conduct set for councillors. If it is reported that there has been a breach of the Code of Conduct then the matter will be referred to the Monitoring Officer in accordance with the procedure and obligations of Councillors to co-operate with any formal standards investigation relating to an alleged breach of this Code.

21.0 Contact Details

21.1 Please contact the Data Protection Officer with enquiries about this Policy.

21.2 Email to: dataprotection@southderbyshire.gov.uk or Telephone: 01283 595795

22.0 Sustainability Impact Assessment

This assessment is completed using the below table. Your assessment should be detailed in the "findings" section. You must detail the reasoning and the mitigation of any negative impacts. If there is 'no impact' no detail needs to be given.

	Positive impact (Y/N)	Negative impact (Y/N)	No impact (Y/N)	Assessment findings
Carbon net zero by 2030/2050	Y			*Please provide information about how the policy interacts with this goal. E.g., how does it reduce or increase carbon emissions? Potential reduction in carbon footprint thorugh regular review and appriorate storage of records with transition to digital where possible.*
Other environmental impacts – waste, biodiversity, etc.			Y	*Please provide information about how the policy interacts with environmental aspects. E.g., what waste is produced and how will it be dealt with, is waste reduced as a part of this policy, how is biodiversity impacted, water use, how will this help communities/staff/businesses to become more environmentally friendly, etc.*

ISO 14001			Y	*How does the policy consider our ISO 14001 EMS, STEMS?* *Does the policy improve or worsen our environmental performance?* *Have any relevant environmental aspects (as per relevant aspect and impact registers) been considered in the writing of the document?*

23.0 Policy Review

23.1 Three years from publication

24.0 References

24.1 Please see Section 6.

25.0 Associated Documentation

Description of Documentation	Document Reference
ICT Security and Acceptable Use Policy	2020 V4
Records Management Policy	2022
Document Retention Policy	2022

26.0 Appendix A

Policy Briefing Form

Introduction

This form is to provide a brief update to summarise the changes/amendments to an existing policy or to provide a summary for a new policy. This form should be used for the consultation, approval and communication of all adopted policies.

Policy update

A summary of the policy is detailed below

Policy Name: Data Protection Policy

Policy Date: April 2026

Version Number: 2.5

Summary of Policy

This policy forms part of South Derbyshire District Council's commitment to the safeguarding of personal data processed by its staff. (Processing has a very broad definition, and includes activities such as creating, storing, consulting, amending, disclosing and destroying data).

Summary of key changes made to an existing policy.

Section	Amendment
All	**Copy to new policy template**

Following final adoption of the policy, this form will be used by the communication team to be included in Core Brief as part of the communication plan.

Further information can be found in the 'My Policies' section in Connect.

27.0 Appendix B

Data Subject	Means a person who is the subject or focus of the personal data.
Personal data	Data which relates to a Data Subject; a living individual who can be identified, either directly or indirectly; a) from those data; or b) from those 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. Personal data gathered may include: Name, age, phone number, address, location, email address, educational background, financial information etc It should also be noted that the definition of personal data is extended to include IP addresses.
Special categories of personal data	Sensitive or Special Categories of Personal Data means personal data consisting of; a) racial or ethnic origin of the data subject b) political opinions c) religious beliefs of other similar beliefs d) trade union membership e) physical or mental health f) sexual life

	g) commission of alleged commission of offences h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings of the sentence of any court in such proceedings. f) genetics g) biometrics (where used for ID purposes)
Criminal Conviction Data	Includes data about; a) The commission of alleged commission of offences; or b) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings of the sentence of any court in such proceedings. Criminal conviction data may relate to a specific crime or legal proceedings but should also be considered as other personal data 'relating to' criminal convictions and offences. It covers any personal data which is linked to criminal offences, or which is specifically used to learn something about an individual's criminal record or behaviour.
Information Asset Owner	An IAO's role is to understand what information is held by their department, what data is being collected and when it will be subject for deletion/destruction as per their retention schedule. They must also know how and where data is transferred and who has access to this data and why. IAO's are responsible for collating this information in information inventories and departmental record management systems.
Data Controller	'Data controller' means a natural or legal person, public authority, agency or other body which, (either alone, jointly or in common with others, determines the purposes and means of the processing of personal data.
Data Processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Legislation	Means the collective term for all UK laws governing the processing of personal data, including the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR), and any subsequent amendments or requirements introduced by the Data (Use and Access) Act and related legislation.

Processing	means obtaining, recording, holding the information or data or carrying out any operation or set of operations on the information or data, including; • organisation, adaption or alteration of the information or data; • retrieval, consultation or use of the information or data; • disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data.
Supervisory authority	This is the national regulatory body responsible for upholding information rights. The supervisory authority for our organisation is the Information Commissioners Office (ICO). The organisation covers legislation including but not limited to: • Data Protection Act and UK GDPR • Freedom of Information Act • Privacy and Electronic Communications Regulations (PECR) • Environmental Information Regulations • The re-use of Public Sector Information Regulations