SOUTH KESTEVEN DISTRICT COUNCIL

South Kesteven District Council
Data Protection Policy

August 2024

Date	Version No:	Revision notes	Author
May 2018	V1	Creation	Lucy Yules
March 2021	V2	The language used has been updated and 10.1 and 10.2 contain updated training requirements.	Stacey Carter
August 2024	V3	1. Additions of the following sections: • Definitions • Aims and Objectives • Roles and responsibilities • Data Breaches • Data Handling • Appeals and Complaints 2. Extra detail added to the following sections. • Introduction • Scope • Data Protection Impact Assessments 3. Removal of section on data Protection principles, now under Appendix 1 4. Addition of Appendix 2 and 3 5. Renumbering of sections 6. Updating of language 7. Updating of relevant links	Niall Jackson

CONTENTS

		Page
Section 1	Introduction	3
Section 2	Definitions	3
Section 3	Scope	3-4
Section 4	Aims and Objectives	4-5
Section 5	Roles and Responsibilities	5-6
Section 6	General Requirements	6
Section 7	Data handling	6-7
Section 8	Information Sharing	7
Section 9	Data Protection Impact Assessments	7-8
Section 10	Data Subject Rights	8
Section 11	Data Retention	8
Section 12	Data Breaches	8-9
Section 13	Transfer to other Countries	9
Section 14	Training	9
Section 15	Information Commissioner Enforcement	9
Section 16	Contact, Information and Guidance	10
Section 17	Non-Compliance	10
Section 18	Appeals and Complaints	10
Section 19	Policy Review	11

1 Introduction

1.1 South Kesteven District Council (the “Council”) processes information about its residents, Members, employees, customers and other data subjects in order to carry its our everyday business and to fulfil its public functions.

1.2 The Council is committed to protecting the rights of all data subjects. Processing of personal data is conducted fairly, lawfully and transparently in accordance with Data Protection Legislation.

2 Definitions

2.1 ‘Personal data’ means any information relating to an identified or identifiable living individual (‘Data Subject’)

2.2 ‘Data Protection legislation' means the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), along with any national implementing laws and secondary legislation as amended or updated from time to time in the UK. This includes any other successor legislation and all other applicable data protection law.

2.3 ‘Identifiable living individual’ means a living individual who can be identified, directly or indirectly, in particular by reference to:

- An identifier such as a name, an identification number, location data or an online identifier
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

2.4 ‘Special category (sensitive) personal data’ means:

- Racial or ethnic origin
- Political opinions
- Religious/philosophical beliefs
- Trade union
- Processing of biometric/genetic data to identify someone
- Health
- Sex life or sexual orientation

2.5 ‘Processing’, in relation to personal data, means an operation or set of operations which is performed on personal data or on sets of personal data, such as:

- Collection, recording, organisation, structuring, storage
- Adaptation or alteration
- Retrieval, consultation, use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination, or
- Restriction, erasure or destruction.

2.6 ‘Data Subject’ means the identified or identifiable living individual to whom personal data relates.

2.7 ‘Controller’ means 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.

2.8 ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2.9 ‘Filing system’ means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

3 Scope

3.1 This Policy applies to:

- All employees of the Council.
- All Members of the Council.
- All Suppliers and Contractors of the Council.
- All Temporary staff engaged by the Council.
- All Volunteers at the Council.
- All Others using the Council's information or systems

3.2 Some of the Council's obligations in this Policy are supported by other policies and procedures. Where relevant, links to those policies and procedures are provided in this document. A list of these can also be found in Appendix 3.

3.3 This Policy relates to personal data, which means any information in paper or digital format relating to a living person who can be identified by that information. Personal data may also be classed as special category data. The definitions of personal and special category data are attached at Appendix 2.

4 Aims and Objectives

4.1 The purpose of this Data Protection Policy is to ensure that the Council adheres to legal requirements, safeguards personal information, and maintains transparency in its data processing practices. The following aims and objectives guide the Council's approach to data protection.

4.2 Compliance with Legal Framework:

4.2.1 The Council's aim is to;

- Comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

4.2.2 The Council's objectives are to:

- Ensure that all data processing activities align with the data protection principles outlined in the GDPR and DPA. These are outlined in Section 6.
- Regularly review and update policies to reflect any changes in legislation.

4.3 Protection of Personal Data:

4.3.1 The Council's aim is to

- Safeguard personal data held by the Council.

4.3.2 The Council's objectives are to:

- Collect, use, and store personal data lawfully and appropriately
- Implement security measures to prevent unauthorised access, loss, or misuse of personal information.
- Educate staff on their responsibilities regarding data protection.

4.4 Transparency and Accountability:

4.4.1 The Council's aim is to:

- Maintain transparency in data processing.

4.4.2 The Council's objectives are to:

- Provide clear privacy notices to individuals regarding how their data is processed.
- Maintain records of data processing activities (data mapping) and make them available for scrutiny.
- Appoint a Data Protection Officer (DPO) to oversee compliance and act as a point of contact for data subjects and the Information Commissioner's Office (ICO).

4.5 Staff Awareness and Training:

4.5.1 The Council's aim is to:

- Ensure that all staff understand their roles in data protection.

4.5.2 The Council's objectives are to:

- Conduct regular training sessions for staff members on data protection principles, rights, and responsibilities.

- Foster a culture of data protection awareness across the Council.

4.6 Risk Management and Accountability:

4.6.1 The Council's aim is to:

- Manage information risks effectively.

4.6.2 The Council's objectives are to:

- Identify and assess risks related to data processing.
- Mitigate risks through appropriate controls and measures.
- Designate a Senior Information Risk Owner (SIRO) responsible for overseeing information risk management.

4.7 Collaboration with External Partners:

4.7.1 The Council's aim is to:

- Ensure secure data sharing.

4.7.2 The Council's objectives are to:

- Establish information sharing agreements with external partners.
- Ensure that data shared externally complies with data protection laws.

4.8 Individuals' Rights and Privacy:

4.8.1 The Council's aim is to:

- Respect individuals' rights over their personal data.

4.8.2 The Council's objectives are to:

- Respond promptly to data subject requests (e.g., access requests, rectification, erasure).
- Promote transparency by informing individuals about their rights.

4.9 By adhering to these aims and objectives, the Council demonstrates its commitment to responsible data handling and protection of individuals' privacy rights.

5 Roles and Responsibilities

5.1 Effective data protection practices rely on clear roles and responsibilities within an organisation. The following roles are crucial for ensuring compliance with legal requirements and safeguarding personal information:

5.2 Data Protection Officer (DPO):

- Email address - (DPO@southkesteven.gov.uk)
- The DPO serves as the primary point of contact for data protection matters within the Council. Their responsibilities include:
  - Providing advice and guidance on data protection laws and regulations.
  - Monitoring compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).
  - Coordinating with relevant departments to ensure data protection policies and procedures are implemented effectively.
  - Handling data breach incidents and reporting them to the Information Commissioner's Office (ICO) when necessary.

5.3 Senior Information Risk Owner (SIRO):

- Name: Richard Wyles
- The SIRO is responsible for overseeing information risk management across the Council. Their duties include:
  - Identifying and assessing information risks related to data processing activities.
  - Ensuring that risk mitigation measures are in place to protect sensitive information.
  - Collaborating with the DPO and other stakeholders to develop and maintain effective data protection practices.
  - Reporting to senior management and the Council on information risk management.

5.4 All Staff Members:

- All employees, contractors, temporary staff, and volunteers have a shared responsibility for data protection. Their duties include:
  - Handling personal data in accordance with established policies and procedures.
  - Reporting any data breaches promptly to the Data and Information Governance Officer, DPO or SIRO.
  - Participating in data protection training and awareness programs.
  - Safeguarding information assets and respecting individuals' privacy rights.

5.5 Council Members:

- Elected Council members play a vital role in ensuring data protection compliance. Their responsibilities include:
  - Advocating for robust data protection practices within the Council.
  - Supporting the DPO and SIRO in their roles.
  - Staying informed about data protection developments and legislation.

5.6 Suppliers, Contractors, and Partners:

- External entities working with the Council must adhere to data protection requirements. Their responsibilities include:
  - Complying with contractual obligations related to data security and privacy.
  - Notifying the Council of any data breaches affecting shared information.
  - Cooperating with the Council during audits or assessments.

5.7 This section outlines the key roles and their associated responsibilities. It is essential that everyone involved understands their part in maintaining effective data protection practices at South Kesteven District Council.

6 General requirements

6.1 The main requirements for data protection are that:

- Personal data will only be accessed by those who need it for work purposes
- Personal data will not be divulged or discussed except when performing normal work duties
- Personal data must be kept safe and secure at all times, including at the office, public areas or in transit
- Personal data will be regularly reviewed and updated
- Internal and external queries about data protection to the Council must be dealt with effectively and promptly

6.2 How the Council complies with these requirements is set out in:

- IT Security Policy http://www.southkesteven.gov.uk/CHttpHandler.ashx?id=24180&p=0
- Acceptable Use of IT Policy http://www.southkesteven.gov.uk/CHttpHandler.ashx?id=24181&p=0
- Protocol relating to the protection of personal data www.southkesteven.gov.uk/CHttpHandler.ashx?id=24183&p=0

7 Data Handling

7.1 Service areas must only collect the minimum amount of personal data that is necessary to fulfil their purposes. Service areas must not collect personal data on the basis that it may be useful, there must be a specific purpose.

7.2 When personal data is collected it must be ensured that the Data Subject is informed who the Data Controller is, the purpose(s) for which the personal data is to be used and any other information about how it will be used or shared. This can, and should, be provided in the form of a privacy notice.

7.3 The IT Security Policy should be adhered to in order to minimise the risk of a data breach.

7.4 Where applicable anonymisation or pseudonymisation techniques should be employed to protect personal data. These techniques should be utilised, when necessary, particularly when sharing personal data with third parties.

7.5 All staff are responsible for ensuring that personal data is used and stored properly to prevent unauthorised access.

7.6 All personal data should:

- Be stored in locked desks or filing cabinets when not in use
- Only be accessed on secure Council equipment and have limited access based on its sensitivity
- Not be visible on screens to unauthorised persons including the public and other members of staff
- Not be taken out of Council offices or stored externally unless such use or storage is necessary and authorised by your line manager
- Only be kept for as long as is necessary and disposed of securely when no longer needed

7.7 All personal data held by service areas should be reviewed at regular intervals and deleted when it passes its retention date unless there are sufficient reasons to extend this period. The reason for holding any personal data passed its retention period should be noted.

7.8 Duplicate records should be avoided to reduce the risk of inaccuracies and anomalies.

8 Information Sharing

8.1 Personal data may need to be shared with other organisations in order to deliver our services or perform our duties. This can only be done where the Council has permission or where there is a legal obligation for us to share personal data.

8.2 Where the Council regularly shares personal information with our partners and other organisations an Information Sharing Agreement will be put in place. This agreement is signed by all partners to the sharing and agrees a set of standards and best practice surrounding Data Protection. However, these are not needed when information is shared in one-off circumstances but a record of the decision and reasons for sharing information will be kept.

8.3 All Data Sharing Agreements will be registered with the Council's Data Protection Officer. That officer will maintain a register of all our Data Sharing Agreements.

8.4 Where the Council shares personal data or gives access to personal data that it holds to anybody acting on its behalf, the Council will require that party to sign a Non-Disclosure Agreement.

9 Data Protection Impact Assessments (DPIAs)

9.1 DPIAs must be completed to help identify and minimise risks to the protection of data in the following situations where personal data is held by the Council:

- At the beginning of a new project or when implementing a new system
- Before entering a data sharing agreement
- When major changes are introduced into a system or process

9.1.1 DPIA's are a means of addressing a projects risk as part of overall project management. They are carried out with a view to identifying and managing any project risks relating to personal data which is collected, used, stored, distributed and destroyed throughout a project.

9.1.2 The function of the DPIA is to ensure that data protection risks are properly identified and addressed wherever possible, and that decision-makers have been fully informed of the risks and the options available for mitigating them. For those proposals that involve data sharing, this could include the risks if data is not shared.

9.1.3 The DPIA will set out information such as, the personal data to be collected, how it will be used, how it will be stored, whether it will be shared and for how long it will be retained.

9.2 For further guidance on undertaking Data Protection Impact Assessments (DPIA's), please read: Procedure for Undertaking a Data Protection Impact Assessment www.southkesteven.gov.uk/CHttpHandler.ashx?id=24187&p=0

10 Data Subject Rights

10.1 The Council is committed to ensuring individuals can freely exercise their rights. Below is a summary of those rights.

- **Right to Access** - This allows the individual to ask the Council if it holds personal information about them, what it uses the information for and to be given a copy of that information. Anyone wanting to know what personal data the Council holds about them can make a Subject Access Request by completing "Subject Access Information Request Form". This form and the procedure for making applications and dealing with SAR's is available on this link: http://www.southkesteven.gov.uk/index.aspx?articleid=8460
- Right to correct incorrect information (rectification) - This means the right to have your personal data corrected if the data we hold is not correct, or completed if it is incomplete. A request for a correction must be made in writing to the Data Protection Officer with proof of identity.
- Right to erasure - This means you have a 'right to be forgotten' and all your personal data deleted in certain circumstances. A request for erasure must be made in writing to the Data Protection Officer with proof of identity.
- Right to restriction of processing of personal data in certain circumstances - This means that you can ask us to limit the way that we use your personal data in some situations. A request for restriction must be made in writing to the Data Protection Officer with proof of identity.
- Right to data portability - This means the right, at your request, to have your personal data transferred from us to another person or organisation, or to use your personal data from somewhere else. A request for portability must be made in writing to the Data Protection Officer with proof of identity.
- Right to object - This means the right to ask that your personal data is not used for profiling, direct marketing, profiling, automated decision-making (for example by a computerised process) and similar uses. An objection must be made in writing to the Data Protection Officer with proof of identity.
- Rights related to automated decision making and profiling - This right enables you to object to the Council making significant decisions about you where the decision is completely automated and there is no human involvement. An objection must be made in writing to the Data Protection Officer with proof of identity.

10.2 The Council aims to acknowledge any requests in relation to the above within 5 working days and provide a substantive response within one calendar month.

11 Data Retention

11.1 Personal Data which is no longer required will be destroyed appropriately. Personal Data will be destroyed in accordance with the Council's retention schedule.

12 Data breaches

12.1 This section should be read alongside the Council's Reporting Personal Data Breaches Policy.

12.2 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

12.3 If any employee or member of the public becomes aware of a breach of the Policy, they should immediately report it to the Data Protection Officer who will be able to advise on any immediate action to be taken. A breach reporting form can be requested from the Data Protection Officer.

12.4 Upon receipt of notification of a breach, the Data Protection Officer will investigate the allegation and, if substantiated, identify an action plan which will include details of containment and recovery action, an assessment of the risks and identify any notifications that need to take place.

12.5 The GDPR requires all organisations to report certain types of personal data breaches to the ICO. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Council will also inform those individuals without undue delay.

12.6 Breaches must be reported to the ICO within 72 hours of the Council becoming aware of the breach.

12.7 The Data Protection Officer will consider the seriousness of the breach, the amount of data, the type of data, the number of customers affected, where the data is now located and whether it is recoverable or not.

12.8 If a Data Subject's personal data is disclosed outside of its intended purpose, they have a right to sue the responsible individual. Individual Officers and Members of the Council may be prosecuted under GDPR, not just the Council as a whole.

12.9 Deliberate breaches will result in disciplinary action under the Disciplinary (Conduct) Policy based on each individual instance.

13 Transfers to other Countries

13.1 Most of our processing occurs in the UK. This means that there are common standards for the processing of personal data that are governed by the ICO.

13.2 Any processing that occurs outside of the UK will need to be assessed and approved by the Data Protection Officer.

14 Training

14.1 Staff training ensures the organisation is compliant with legislative requirements and provides employees with the knowledge of their responsibility to keep personal data secure.

14.2 All employees must complete Data Protection training annually (including temporary employees). Members will complete Data Protection awareness sessions at Member Induction. They will also be offered Data Protection training within the Members Development Programme.

15 Information Commissioner Enforcement

15.1 The Information Commissioner has various enforcement powers at its disposal ranging from inquiries into data breaches, Information Notices, Assessment Notices, Enforcement Notices, Powers of Physical Entry and Inspection, and ultimately, Penalty Notices and Prosecution.

15.2 Penalty notices or monetary penalties (fines) may be served for noncompliance with the DPA and serious data breaches. There are two levels as follows:

- The "higher maximum amount" is 17.5 million Pounds, or 4% of the organisation's annual revenue from the preceding financial year, whichever amount is higher.
- The "standard maximum amount" is 8.7 million Pounds, or 2% of the organisation's annual revenue from the preceding financial year, whichever amount is higher.

15.3 The maximum amount of penalty in sterling will be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

15.4 The "higher maximum" will apply to very serious and or damaging data breaches that fail to comply with the fundamentals of the DPA principles.

15.5 All fines are made public by the Commissioner and the Chief Executive of the offending organisation is usually asked to make a formal undertaking to put in place effective measures and remedies.

15.6 If the organisation disputes the fine, it can appeal to the First-Tier Tribunal within 28 days of being informed of the Monetary Penalty Notice.

16 Contact, Information and Guidance

16.1 Requests for any information relating to rights or data protection matters should be made in writing to:

The Data Protection Officer
South Kesteven District Council
The Picture House
St Catherines Road
Grantham
Lincs
NG31 6TT
Email: dpo@southkesteven.gov.uk

16.2 Information can also be obtained from the Information Commissioner at:

The Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
https://ico.org.uk
Telephone 0303 1231113 (local rate) or 0162 5545745 (national rate)

17 Non-Compliance

17.1 Individual members of staff can face disciplinary action for misusing personal data. Malicious misuse and unauthorised disclosure of personal data can also lead to personal prosecution and/or liability to pay compensation in any civil action.

17.2 Elected Members when handling personal data in relation to Council business must comply with this Policy. Malicious misuse and unauthorised disclosure of personal data can also lead to personal prosecution and/or liability to pay compensation in any civil action.

18 Appeals and Complaints

18.1 Where an applicant is dissatisfied with the level of service they have received, they are entitled to complain about the actions of the Council through the internal appeals procedure. All complaints should be forwarded to feedback@southkesteven.gov.uk

18.2 The applicant will receive a response to their correspondence within twenty working days. If the applicant remains dissatisfied with the Council's reply, they have the option of taking their complaint to the Information Commissioner (at the address below) who will independently adjudicate each case and make a final decision.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

19 Policy Review

19.1 This Policy will be reviewed every two years or where significant changes to legislation occur.

19.2 Reviews of this Policy will take into account changes in the law, best practice, lessons learnt and changes in information technology (IT).

19.3 The most current version of this document will be made available on the Councils website for viewing.

APPENDIX 1

DATA PROTECTION PRINCIPLES

Lawfulness, Fairness, and Transparency:

- Ensure that data is obtained and processed fairly and lawfully.
- Be transparent by providing an easy-to-understand privacy Policy that details what data you collect and how you plan to use it.

Purpose Limitation:

- Collect personal data only for specific purposes and use it solely for those purposes.
- Clearly communicate the purposes or uses of the data.

Data Minimization:

- Collect only the necessary data; avoid excessive or irrelevant information.
- Ensure that the data you collect is adequate and relevant for the intended purpose.

Accuracy:

- Keep personal data accurate and up to date.
- Implement processes to verify and correct any inaccuracies.

Storage Limitation:

- Define how long you will retain personal data.
- Regularly review and delete data that is no longer necessary.

Integrity and Confidentiality (Security):

- Implement appropriate security measures to protect the data you collect and process.
- Regularly test and update security protocols.

Accountability:

- Demonstrate compliance with GDPR regulations.
- Maintain records of processing activities and be prepared to respond to regulatory investigations

Appendix 2

PERSONAL DATA

Is identified by Article 4 of the GDPR as “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 CATEGORY DATA (SENSITIVE PERSONAL DATA)

Is identified by Article 9 of the GDPR as “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of generic 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.”

Special Category Data can only be processed by the Council if one or more specified statutory conditions apply. The statutory conditions are set out in summary below:

- Explicit consent (unless law prohibits the processing, and that prohibition cannot be overridden by the person)
- Legal obligation on the controller in respect of employment, social security etc.
- Protection of the vital interests of the data subject or another person where the data subject is legally or physically incapable of giving consent
- Legitimate activities of a non-profit making organisation with a political, philosophical or trade union aim
- The personal data is manifestly made public by the data subject
- Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Substantial public interest (based on a Union or State law which is proportionate to the aim pursued, respects the essence of the right to data protection and provides specific measures to protect the fundamental rights and freedoms of the data subject)
- Necessary for the purposes of preventative or occupational medicine, assessment of working capacity, medical diagnosis, provision of health or social care or treatment or the management of health and social care systems and services on the basis of Union or State law
- Public health (on the basis of Union or State law)
- Archiving in the public interest, research and statistics.

Appendix 3

LINKED POLICY AND PROCEDURES

- Procedure for Undertaking a Data Protection Impact Assessment
- Procedure for reporting Information Security Breaches Data Protection Breaches and Card Data Security Incidents
- Breach reporting form
- Information Governance Guidance
- Protocol for protecting personal data
- IT Security Policy
- Acceptable use of IT Policy