South Kesteven District Council

Data Protection Policy

June 2018

SOUTH KESTEVEN DISTRICT COUNCIL

CONTENTS

1 Introduction

1.1 This is South Kesteven District Council's Data Protection Policy.

1.2 South Kesteven District Council processes personal data to carry out its duties and obligations. This policy sets out the Council's commitment to protecting and handling personal data.

2 Scope

2.1 This Policy applies to:

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

2.2 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.

2.3 This policy relates to personal data, which means any information in paper or digital format relating to a person who can be identified by that information. Personal data may also be classed as special category (sensitive) data. The definitions of personal and special category (sensitive) data are attached at Appendix 1.

3 Data Protection Principles

3.1 South Kesteven District Council must protect and process the personal data, which it holds in accordance with data protection principles established by law. The Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR), require us to be sure that all personal data is:

- Processed fairly, lawfully and in a transparent manner ('lawfulness, fairness and transparency');

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

- Adequate, relevant and limited only to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- Accurate and where necessary kept up to date, erased or rectified without delay ('accuracy');

- Kept in a form which permits identification of data subjects for no longer than is necessary ('storage limitation');

- Processed in accordance with the rights of data subjects

- 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 ('integrity and confidentiality').

4 General requirements

4.1 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

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

and the Protocol relating to the protection of personal data
www.southkesteven.gov.uk/CHttpHandler.ashx?id=24183&p=0

5 Information Sharing

5.1 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 we have permission or if there is a legal obligation for us to share personal data.

5.2 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.

5.3 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.

5.4 Where we give personal data or give access to personal data that we hold to anybody acting on behalf of the Council, we will require that party to sign a Non-Disclosure Agreement.

6 Privacy Impact Assessments (PIAs)

6.1 PIAs will 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

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

7 Data Subject Rights

7.1 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

8 Data Retention

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

9 Transfers to other Countries

9.1 Most of our processing occurs in the UK or European Union. This means that there are common standards for the processing of personal data.

10 Training

10.1 Data Protection training is important so that we can be sure that all employees and agency workers understand their responsibilities. All employees (including temporary employees) will complete Data Protection training every year and Elected Members will be offered the same training.

11 Information Commissioner Enforcement

11.1 The Information Commissioner has various enforcement powers at it's 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.

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

- The "higher maximum amount" is 20 million Euros (£17.6m)
- The "standard maximum amount" is 10 million Euros (£8.8m)

11.3 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.

11.4 The "higher maximum" will apply to very serious and or damaging data breaches and fundamental failure to comply with the fundamentals of the DPA ideals.

11.5 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.

11.6 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.

12 Contact, Information and Guidance

12.1 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
Council Offices
St Peters Hill
Grantham
Lincs
NG31 6PZ Email: dpo@southkesteven.gov.uk

12.2 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)

13 Non Compliance

13.1 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.

13.2 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

14 Policy Review

14.1 This policy will be reviewed annually.

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

APPENDIX 1

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, 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.