SOUTH KESTEVEN DISTRICT COUNCIL

CABINET

Report of: Councillor Kelham Cooke,
The Deputy Leader of the Council

Report to:	**Cabinet**
Date:	**6th September 2018**
Subject:	**Data Protection Policy** **Report Number: LDS309**

Decision Proposal:	Key Decision
Relevant Cabinet Member:	Councillor Kelham Cooke, The Deputy Leader of the Council
Report author:	Mandy Braithwaite Legal Executive Tel: 01476 406106 E-mail: m.braithwaite@southkesteven.gov.uk Date: 2.8.18
Reviewed by:	Lucy Youles Solicitor to the Council Tel: 01476 406105 E-mail: l.youles@southkesteven.gov.uk Date: 3.8.18
Signed off by:	Debbie Muddimer, Strategic Director - Resources Tel: 01476 406301 Email:debbie.muddimer@southkesteven.gov.uk Date: 7.8.18
Approved for publication	Councillor Kelham Cooke Date: 7.8.18

SUMMARY
The report sets out the Council's policy and procedures relating to data protection in line with data protection legislation which was enacted on the 23rd May 2018. The draft Data Protection Policy and supporting documents are attached as the Appendices to this report.

RECOMMENDATION

It is recommended that:

1. Cabinet approve the draft Data Protection Policy as attached to this Report at Appendix 1.

1. BACKGROUND TO REPORT

1.1 The Data Protection Policy was last revised in 2015. The policy must now be reviewed and updated following the introduction of the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

1.2 The Council holds the personal data of all its customers and people who interact with the Council. The Council, as a data controller, must make sure that the personal data which is received, processed, retained and shared is protected in accordance with the legal framework. The purpose of the draft policy is to set out for the benefit of members of the public, Council officers, Members of the Council and third parties with whom the Council engage, how the Council will protect the personal data which it processes.

1.3 The Data Protection Act 1998 has been replaced by the Data Protection Act 2018 which implemented the GDPR into UK law on 25 May 2018. The Council should adopt a policy to enable it to show how it will protect personal data in accordance with the new framework.

1.4 Many of the GDPR's main concepts and principles are the same as those in the previous data protection legislation. The GPDR has introduced increased rights for individuals, tighter time limits for reporting breaches and increased fines for breaching data protection legislation and associated powers of the Information Commissioner.

1.5 The draft Data Protection Policy is attached to this report at Appendix 1. Several procedure documents have been drafted to compliment the policy and will be available as links within the policy. These are:

- Appendix 2 - Subject Access Request Procedure
- Appendix 3 – Procedure for Data Protection Impact Assessments
- Appendix 4 – Generic Privacy Notice
- Appendix 5 – Breach Procedure
- Appendix 6- Protocol for Protecting Personal Information
- Appendix 7 – Information Governance Guidance

1.6 The draft Data Protection Policy and related procedures have been considered by the Communities and Wellbeing Overview and Scrutiny Committee and has recommended that the Cabinet approve the policy as drafted.

2 OVERVIEW OF CHANGES

2.1 <u>The Data Protection Principles</u>

2.1.1 The GDPR states that anyone processing personal data must apply the six data protection principles:

Lawfulness, fairness and transparency principle - personal data must be processed fairly, lawfully and in a transparent manner.

Purpose limitation principle - personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those processes;

Data minimisation principle - personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

Accuracy principle – the personal data collected must be accurate and where necessary kept up to date**;**

Storage limitation principle - the data should only be kept in a form which permits identification of an individual for no longer than is necessary for the purpose for which the data is processed;

Integrity and confidentiality principle - personal data must be processed in a manner that ensures appropriate security to protect against unauthorised processing, loss, destruction or damage.

2.2 Legal Basis for Processing

2.2.1 The Council can process personal data in accordance with a legal basis. These are:

- The processing is necessary to fulfil or prepare a contract for the individual;
- There is a legal obligation to process the data;
- Processing the data is necessary to protect a person's life or in a medical situation;
- Processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law;
- The processing is necessary for legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest;
- We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.Such consent must involve clear affirmative action. Consent can no longer be inferred. The Council is required to keep clear written records to demonstrate that consent has been given by an individual. A person will also have the right to withdraw consent. The Council is required to inform individuals of their right to withdraw consent.

2.3 Individual Rights

2.3.1 The Council, as a data controller, is required to process personal data in a transparent manner. To ensure this happens, the GDPR has introduced the following rights for individuals:

- The right to be informed of the collection and use of personal data. This right will be published in privacy notices (see Appendix 4 and paragraph 6 below) ;
- The right to request that inaccurate personal data is rectified;
- The right to request that personal data is erased;
- The right to request that processing of personal data is restricted;
- The right to data portability which allows individuals to obtain and reuse their data across different Council services;
- The right to object to the processing of personal data;
- The right not to be the subject of automated decision making including profiling.

2.3.2 All the above rights are in addition to the existing right to individuals to access the personal data held about them by the Council (subject access request). The timescale for complying with such a request has reduced from 40 days to 30 calendar days. There is no longer a fee payable for this request or for any of the rights referred to above. The procedure for making and processing a subject access request is detailed in the Subject Access Request Procedure attached to this report at Appendix 2

2.4. Data Protection Impact Assessments (DPIA)

2.4.1 A DPIA is a process to help identify and minimise the data protection risks of Council projects and actions which involve the processing of personal data. The GDPR requires the Council to carry out a DPIA if it plans to for example:

- Install CCTV cameras;
- Process sensitive personal data on a large scale;
- Process personal data that might endanger an individual's health or safety in the event of a security breach;
- Process personal data that concerns vulnerable adults or children.

2.4.2 A procedure for carrying out a DPIA has been drafted and is attached as Appendix 3 to this report.

2.5. Privacy Notices

2.5.1 Individuals have a right to be informed about the collection and use of personal data. This is a transparency requirement of the GDPR. This can be done by way of a privacy notice. The information required in a privacy notice includes the purposes of the processing, the legal basis for the processing, the period for which the personal data will be stored and the individual's rights relating to the processing of personal data.

2.5.2 A generic privacy notice has been drafted which is attached to this report as Appendix 4. It is proposed that each service which processes personal data will provide a specific privacy notice relating to the processes of that service. These privacy notices are currently being prepared.

2.6 Record of Processing Activities

2.6.1 The Council is currently carrying out a process of recording its data processing activities. This involves each service of the Council responding to a series of

questions relating to personal data collected and how it is used. This record will be used to review processes and ensure that personal data is being processed in accordance with the legislation.

2.7. Data Protection Breaches

2.7.1 The Council is required to report to the Information Commissioner notifiable breaches of data protection within 72 hours of a breach occurring. A potential breach procedure has been drafted and is attached to this report as Appendix 5.

2.7.2 The GDPR has introduced new levels of fines for failure to notify a breach of up to £8.8m. Fines of up to £17.6m may be imposed for the actual breach.

2.7.3 The Data Protection Act 2018 introduces offences;

- for the deliberate or reckless obtaining, disclosing, procuring and retention of personal data without the consent of the data controller;
- knowingly or recklessly re-identifying data which has been de-identified; and
- Alteration of personal data to prevent disclosure in respect of a subject access request.

These offences apply to any person processing personal data on behalf of the Council.

3 TRAINING AND AWARENESS

3.1 The document "the Protocol for Protecting Personal Information" has been produced and is attached to this report at Appendix 6. This document will be available as a link within the Data Protection Policy. This is intended to assist those processing personal data to avoid potential breaches of data protection. In addition, all employees of the Council are required to carry out on-line data protection training. Further training is proposed following the adoption of the proposed draft policy.

3.2 Information Governance guidance is produced at Appendix 7. This document sets out the various roles and responsibilities of officers, Members of the Council and third parties acting on behalf of the Council.

4. OTHER OPTIONS CONSIDERED

4.1 There are no other options to consider.

5. RESOURCE IMPLICATIONS

5.1 All services within the Council have been involved in the recording and mapping of personal data processing to ensure compliance with GDPR. This work will continue as part of the day to day procedures of the Council. Budgetary provision has been made for the engagement of a Data Protection Officer which is a requirement of the Data Protection Act 2018.

6. RISK AND MITIGATION

6.1 The Data Protection Policy and associated documents are intended to reduce the risk of data breach and non-compliance with the legislation.

7. ISSUES ARISING FROM IMPACT ANALYSIS (EQUALITY, SAFEGUARDING etc.)

7.1 No impact analysis is required.

8 CRIME AND DISORDER IMPLICATIONS

8.1 Malicious misuse of personal data processed by the Council could lead to prosecution of individuals.

9. COMMENTS OF FINANCIAL SERVICES

9.1 It is imperative that the legislation and policy relating to data protection is followed to avoid the imposition of penalties which could have a major financial impact on the Council

10. COMMENTS OF LEGAL AND DEMOCRATIC SERVICES

10.1 The Council must implement a policy which is compliant with the GDPR and the new Data Protection Act 2018. Privacy notices must be published, procedures put in place, records maintained and appointments made in accordance with the new legislation.

11. COMMENTS OF OTHER RELEVANT SERVICES

11.1 None

12. APPENDICES

12.1 Appendix 1 – Draft South Kesteven Data Protection Policy
Appendix 2 – Subject Access Request Procedure
Appendix 3 – Procedure for Data Protection Impact Assessments
Appendix 4 – Generic Privacy Notice
Appendix 5 – Breach Procedure
Appendix 6- Protocol for Protecting Personal Information
Appendix 7 – Information Governance Guidance

13. BACKGROUND PAPERS

13.1 Data Protection Act 2018 –
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

IT Security Policy http://intranet/CHttpHandler.ashx?id=16922&p=0

Acceptable Use of IT Policy http://intranet/CHttpHandler.ashx?id=16916&p=0
Current Data protection Policy