South Somerset District Council

Data Protection Policy

Version Details:

Version:	2.0
Date:	29/09/20
Service:	Strategy & Commissioning
Author:	Cath Temple
Review Date:	January 2021

South Somerset District Council

Introduction:

The General Data Protection Regulations came into effect on 25th May 2018. In meeting the requirements of GDPR and The Data Protection Act (DPA) 2018, South Somerset District Council(SSDC) undertakes to ensure that personal data is:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals
b) Collected for specified, explicit and legitimate purposes and not further processed in any manner that is incompatible with those purposes
c) Adequate, relevant and limited to what is necessary in relation to the purposed for which they are processed
d) Accurate and up to date. Every reasonable step will be taken to ensure that personal data that isn't correct will be rectified and that which requires deletion is actioned without delay.
e) Not kept for longer than is necessary
f) 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

In addition, we take responsibility for complying with the accountability principle in that we demonstrate that we follow the above principles.

Purpose

South Somerset District Council regards the lawful, accurate and correct treatment of personal information important in maintaining the confidence of those with whom we deal and for successful operations.
We will always do our utmost to ensure that our organisation treats personal information lawfully and correctly.

We fully endorse and adhere to the Data Protection Act 2018 and the General Data Protection Regulations 2018 and this policy outlines the steps we take to ensure we are complete with them, that we implement and adhere to them.

Definitions

The GDPR refers to "Controllers" **and** "Processors. A Controller determines the purposes and means of processing personal data, whilst a Processor is responsible to processing personal data on behalf of a Controller.

- SSDC will variously take the role of Processor and/or Controller. As Processor, the GDPR places specific legal obligations on us; for example, we are required to maintain records of personal data and processing activities.

- Where others process data on our behalf, the GDPR places further obligations on us to ensure our contracts with Processors comply with GDPR.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The GDPR refers to sensitive personal data as "special categories of personal data"; for example, information about an individual's:

- Race;
- Ethnic origin;
- Political views;
- Religious beliefs;
- Trade union membership;
- Genetics;
- Biometrics (where used for ID purposes);
- Health data;
- Sex life; or
- Sexual orientation

Special category data is personal data which is more sensitive and therefore requires more protection.

Specific responsibilities

Data Protection Officer – there is a data protection officer at South Somerset District Council (DPO@southsomerset.gov.uk) who:

- Is registered with the Information Commissioners Office (ICO);
- Maintains an Information Asset Register (IAR) – a register of databases held by SSDC which contain personal data
- Monitors and reports on the processing of Subject Access Requests
- Ensures SSDC's ability to meet the requirements of DPA 2018 and GDPR organisationally and technically
- Audit's the Council's compliance with this policy and report to the Senior Leadership Team any complaints in respect of data privacy
- Reports any relevant data breaches to the Information Commissioners Office
- Ensures that training in GDPR is undertaken by **ALL** Officers and Members and is kept up to date.
- Oversees and reports on the processing of Freedom of Information requests

Information Asset Owners – it is the responsibility of each information asset owner to:

- In cases where we process personal data for any other reason than that for which it was collected, the Information Asset Owner must bring this to the attention of the individual BEFORE the processing can start
- Inform the Data Protection Officer (DPO) of any changes or additions to the Information Asset Register
- Ensure the data custodians assigned to their databases are made aware of the standards applicable to their datasets and monitor their adherence
- Be aware of their responsibilities in respect of processing that data only for the purposes specified when it was collected
- Ensure our contracts with Processors comply with DPA2018 and GDPR
- Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, ensure that the breach is communicated to the data subject(s) without undue delay
- Raise a breach report immediately in the event of a personal data breach

Data Custodians – it is the responsibility of everyone at SSDC to:

- Provide individuals with privacy information at the point we collect any personal data and via all possible channels in the form of a **Privacy Notice**
- Pass any Freedom of Information (FOI) requests to the FOI Team (FOI@southsomerset.gov.uk) to ensure that they are all dealt with in a timely manner. It is our statutory duty to investigate and respond to FOIs within 20 working days. We aim to publish all completed requests on the SSDC website.
- If FOI requests look likely to exceed the 18-hour time limit, inform the DPO as soon as possible.
- When Subject Access Requests (SAR) are made over the phone, letter or face-to-face, the Officer will signpost the individual to the dedicated email account (SAR@southsomerset.gov.uk) or raise the request on behalf of the individual, making sure that we have the correct details of the request and address where the response is to be sent
- In the case of a data breach, capture the details and complete a breach report form via the portal. Even if you aren't sure if personal data is involved, raise the form and the DPO can investigate further, contacting you where required.
- For all data protection queries, no matter how big or small, send an email to DPO@southsomerset.gov.uk wherever/whenever you feel a breach has occurred. This is accessed via the

Case Team, Strategy & Commissioning, will;

- On receiving a SAR, take appropriate action and respond to the individual notifying them of the statutory timescales involved (1 calendar month)
- Verify the identity of the person making the request
- Respond to requests in a suitable format, e.g. if request has come via email, respond accordingly

- Provide information in a form which is concise, transparent, intelligible, easily accessible and it must use clear and plain language
- If the SAR relates to rectification, make a note on relevant system(s) indicating that the individual challenges the accuracy of the data and their reasons for doing so, also that we will restrict processing of the personal data in question whilst we are verifying its accuracy
- Restrict processing in cases where we are considering accuracy or the legitimate grounds for processing any personal data in question. This will be marked on appropriate systems.
- Where we have disclosed personal data to any other body, any actions taken in respect of that data will be communicated to the individual, where it is appropriate. For example, this would not be the case if the individual was being investigated for fraud, informing them could potentially harm any investigation therefore informing them would not happen in this case.
- Where requests are received for data to be transported, we will provide it in a structured, commonly used and machine readable format. The information must be provided free of charge.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project. We will complete a DPIA for processing that is likely to result in a high risk to individuals. It is good practice to complete a DPIA for any other major project which request the processing of personal data. The DPIA template is available from DPO@southsomerset.gov.uk and covers the following:

- Description of the nature of processing, scope, context and purposes of processing;
- Assess necessity, proportionality and compliance measures;
- Identification and assessment of risks to individuals; and
- Identification of additional measure to mitigate risks

To assess the level of risk, you must consider both the likelihood and severity of any impact on individuals, using our Risk Management Framework. High risk could result from either a high probability of some harm or a lower possibility of serious harm. Complete the form and consult with the DPO and/or relevant experts.