Data Protection Policy

Opening statement

South Staffordshire District Council ('the Council') is committed to complying with data protection legislation. This includes the UK version of the General Data Protection Regulation 2016, the Data Protection Act 2018 and the Privacy and Electronic Communication Regulations 2003.

This policy sets out the Council's approach (primarily through its employees and members) to the handling of personal data.

As a Council we recognise that the correct and lawful treatment of people's personal data will maintain their confidence in us and will provide for successful operations.

Protecting the personal data of individuals is something that the Council takes extremely seriously. The Council is potentially exposed to substantial (£17 million or 4% of its annual revenue/turnover - whichever is greater) fines depending on the nature and severity of the infringement for failure to comply with data protection legislation.

Anyone who processes personal data on behalf of the Council such as employees, members, contractors and suppliers must comply with this policy. For ease of reading the above categories will be referred to simply as 'employees' in the rest of this policy.

Compliance with this policy is mandatory. Related policies and procedures/guidelines are available to assist employees in complying with legislation.

Any breach of this policy or the related policies and procedures/guidelines may result in disciplinary action, termination of contracts or action under the Council's Code of Conduct

This policy applies to all personal data the Council processes regardless of the media on which that data is stored.

The law (and this policy) applies to:

1. Personal data processed by automated means such as computers, phones, tablets, CCTV, swipe cards etc. or,
2. (structured) personal data held in a 'relevant filing system' for example an employee's personnel file or it is intended to form part of such a file or,
3. unstructured personal data such as paper records that are not held as part of a filing system.

Data Protection Policy

Definitions

The following expressions are used in this policy:

Personal data - this is any information relating to an identified or identifiable (from information in the possession of the Council or when put together with other information the Council might access) living individual.

Special category personal data is that about an individual's race/ ethnicity, political opinions, religious or philosophical beliefs, membership of a trade union, their genetic/ biometric data (if used to identify them), health information or information about their sex life or sexual orientation.

Processing includes receiving information, storing it, considering it, sharing it, destroying it etc.

A Processor is a third-party individual/organisation who process personal data on the Council's behalf -to its instructions.

The Council is the Controller of people's personal data as it determines what is collected, why and how it is used.

Consent means any freely given, specific, informed and unambiguous indication of a person's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

A data breach means a breach of Council security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Commitment to the principles

The Council MUST:

(a) process personal data fairly, transparently and only if there is a legal basis to do so.

To comply with this, employees must provide individuals when collecting their personal data (concisely and using clear and plain language so that they understand) with the following information:

1. that the Council is the "controller" of their personal data;
2. the Council's contact details;
3. why the Council is processing their personal data and in what way the law allows it;
4. if the Council [this will be rare] relies on its 'legitimate interests' or those of a third party for processing personal data what those interests are;
5. the identity of any person/ organisation to whom their personal data may be disclosed;
6. whether it is intended to process their personal data outside the United Kingdom;
7. how long their personal data will be retained for; and,
8. their rights.

[more information is given on the next page]

Privacy information should be tailored to the recipient so that they clearly understand what is happening with their data and their rights.

(b) only collect personal data for specified, explicit and legitimate purposes.

Employees must not further process any personal data in a manner that is incompatible with the original purposes; Employees should be clear as to what the Council will do with a person's personal data and only use it in a way they would reasonably expect.

(c) ensure that the personal data it collects is adequate, relevant and limited to what is necessary to carry out the purpose(s) it was obtained for;

Employees should think about what the Council is trying to achieve in collecting personal data. Employees must only collect the personal data that they need to fulfil that purpose(s) and no more. Employees must ensure that any personal data collected is adequate and relevant to the intended purpose(s).

(d) ensure that the personal data it processes is accurate and, where necessary, kept up to date.

Employees must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Employees must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

(e) keep personal data in a form that identifies individuals for no longer than is necessary for the purpose(s) that it was obtained.

Employees should periodically review what personal data is held and erase/destroy or anonymise that which is no longer needed.

(f) process personal data (whatever the source) in a manner that ensures appropriate security of the same including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This is elaborated upon in the Council's information security policy/procedures/guidelines.

Accountability

The Council is responsible for and must be able to demonstrate that it complies with all the above principles. Employees should always be mindful of the need to be able to prove that processing is in accordance with the above principles.

Legal basis for processing ordinary personal data (article 6)

The Council (through its employees) must process personal data ONLY if one or more of the following circumstances exist:

a. Where an individual has given valid [see definition] consent;
b. Where necessary to perform a contract to which the individual is a party or to take steps at their request prior to entering into a contract;
c. Where processing is necessary for the Council to comply with its legal obligations;
d. Where processing is necessary for the performance of a task carried out in the public interest by the Council or it is in the exercise of official authority vested in the Council;
e. To further the Council's [this will be rare] legitimate interests or those of a third party except where such interests are overridden by the privacy interests of the individual who is the subject of the information especially if they are a child.

****Employees must always ensure that they have a lawful basis to process personal data on behalf of the Council before they process it. No single basis is 'better' or more important than the others. Employees should consider and document what basis they are processing the personal data under. If an employee is unsure as to what basis they can rely upon then the advice of the Data Protection Officer should be sought****

Special category personal data (article 9)

The Council (through employees) MUST not process this kind of information unless circumstances exist such as:

a. the individual has given explicit consent for one or more specified purposes;
b. it is necessary for employment/ social security/ social protection law purposes;
c. it is necessary in relation to legal claims, or,
d. it is necessary for reasons of substantial public interest.

Other grounds are potentially available.

****Again, if an employee is unsure as to how to lawfully process special category personal data, then the advice of the Data Protection Officer should be sought****

Criminal offence data

To process personal data about criminal convictions or offences, the Council must have a lawful basis under article 6 (above) and legal authority or official authority. For further advice speak with the Data Protection Officer.

Data protection rights

Individuals have rights when it comes to how the Council handles their personal data. These include rights to:

a. withdraw consent to processing at any time;
b. receive certain information when the Council collects their information or receives it from a third party;
c. request access to their personal data;
d. have the Council correct inaccurate information;
e. ask the Council to erase their personal data;
f. restrict the way the Council uses their information;
g. be notified about any recipients of their personal data when they have asked for rectification, erasure or restriction;
h. object to any processing undertaken by the Council in the public interest/exercise of official authority or its legitimate interests or those of another;
i. object to direct marketing by the Council, and, to
j. be notified by the Council of a personal data breach where it is likely to result in a "high risk" to their rights and freedoms.

Rights are not absolute. They are fact specific. They should normally be dealt with within a month of receipt and free of charge. Procedures exist (which should be followed) if a person seeks to exercise any of the above rights. If an employee receives a request by an individual to exercise a right the advice of the Data Protection Officer should be sought.

Restrictions

In certain circumstances the Council is permitted to restrict the above rights and its obligations as well as depart from the principles. Any restriction will be in accordance with the law. For further advice speak with the Data Protection Officer.

Data protection by design and default

Considering available technology, the cost of implementation of it and the nature, scope, context and purposes of the processing as well as the privacy risks to individuals the Council MUST both at the time it decides how to process personal data and at the time of the processing itself, implement appropriate technical and organisational measures (such as pseudonymisation) so as to ensure that any processing is in accordance with the law. This is to protect the privacy of individuals.

The Council must also implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing activity are processed. That obligation applies to the amount of personal data collected, the extent of the processing, the period of storage and its accessibility to individuals.

****For any new projects that involve the processing of personal data the advice of the Data Protection Officer must be sought, no later than the commencement of the project planning stage, so that compliance with data protection law can be built in at the earliest opportunity. ****

Joint controllers

Where the Council and another controller jointly determine why and how personal data should be processed the Council will be regarded as a 'joint controller'. If this is the case,then the appropriate employee must work with their 'opposite number' to determine the respective responsibilities of the controllers for compliance with the GDPR, for instance the exercise of any rights by an individual and the controllers' respective duties to provide privacy information. The arrangement must reflect the respective roles and relationships of the joint controllers towards the individual(s). The essence of the arrangement should be made available to any individual.

Council use of data processors

These are external people/organisations who process personal data on the Council's behalf to its order.

Employees MUST ensure that any processor it is proposed to use:

a. has provided sufficient guarantees of having implemented appropriate technical and organisational measures to satisfy the Council that personal data will be processed in accordance with the law and,
b. that it will not engage another processor without the Council's written authorisation.

In addition, any processing MUST be governed by a contract that is binding on the processor. It should set out the subject-matter and duration of the processing, nature and purpose of the processing and the type of personal data and categories of individuals.

The contract MUST set out that:

a. The processor will only process the personal data on documented instructions from the Council.
b. Any person or organisation authorised to process personal data have committed themselves to confidentiality.
c. That the processor puts in to place appropriate security measures.
d. The processor assists the Council in meeting its obligations as regards requests by people to exercise their data protection rights.
e. The processor assists the Council in complying with its personal data security obligations, notifications to the Information Commissioner's Office and to affected individuals and in respect of Data Protection Impact Assessments.
f. The processor deletes or returns all personal data to the Council after the end of the provision of the processing services.
g. The processor makes available to the Council all information necessary to demonstrate compliance with the above and to allow for and contribute to audits, including inspections etc.

Records of processing activities

The Council is obliged to maintain a record of its processing activities. The record will contain, amongst other matters, information about:

a. why the Council processes personal data;
b. the categories of individuals whose personal data is processed and the categories of personal data;
c. the categories of recipients to whom personal data have been or will be disclosed to;
d. the envisaged time limits for erasure of the different categories of data;
e. (generally) the technical and organisational security measures that the council has in place.

****If employees are aware of any changes in the above, they should inform the Data Protection Officer who will make the required changes to the record****

Personal Data Breaches

In certain situations, the Council will be obliged to report breaches to the Information Commissioner's Office and affected individuals.

All suspected or actual breaches must be reported to the Data Protection Officer using the report form available on The Core as soon as an employee becomes aware of it. The Data Protection Officer will acknowledge receipt of the report and will, where appropriate,liaise with other employees such as ICT, public relations, insurance and legal in responding to the breach. Any report to the ICO (which should be within 72 hours of discovery of the breach) or to affected individuals will be upon the authority of the Chief Executive or their Deputy in their absence.

Any report to the ICO will provide:

- a description of the personal data breach
- a description of steps taken as a consequence of a breach
- the contact details of the DPO, or other point of contact
- a description of measures taken to mitigate any possible breaches

Any breaches reported to the Data Protection officer will also be recorded on the Council's Personal Data Breach register.

Data Protection Impact Assessments

Where a type of processing of personal data, using new technology, and considering the nature, scope, context and purposes of the processing, is likely to result in a high risk to the privacy of individuals then employees MUST prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the individuals. As part of this process employees MUST seek the advice of the Data Protection Officer.

Data Protection Officer (DPO)

The Council's designated DPO is Lorraine Fowkes. The DPO MUST be involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The Council will support the DPO in performing her [this list is not exhaustive] tasks which are:

a. to inform and advise the Council of its legal obligations under all data protection laws;
b. to monitor the Council's compliance with GDPR and other data protection laws and the Council's compliance with its internal policies and procedures and to assign responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;
c. to provide advice were requested about any data protection impact assessment and monitor its performance;
d. to cooperate with the Information Commissioner;
e. to act as the contact point for the Information Commissioner on issues relating to the processing of personal data, including data protection impact assessments and consultations and where appropriate, any other matter.

Transfers outside the United Kingdom

If an employee proposes to send personal data outside of the UK, then the advice of the DPO should be sought before transfer to ensure that it is done so lawfully.

Marketing

Employees must ensure that they always have a legal ground under the GDPR to market to individuals. Where marketing is carried out electronically (text, email etc.) then employees must adhere to the privacy regulations (2003) and ensure that they have consent unless the 'soft' opt-in applies e.g., when signing up for a council service such as leisure membership or green waste. Further advice can be sought from the DPO.

Further information

CLT are responsible for ensuring that this policy and the related documents are complied with. However, if you have any questions about the policy or data protection generally, please speak with the Data Protection Officer.

Changes to this policy

The Council reserves the right to change this policy at any time. If it does, it will draw any changes to the attention of employees.

Version 2

Review date (by) 1 November 2023

[Checked CN Wolves]