South Norfolk Council

Data Protection Policy

CONTENTS

1. Policy Statement

1.1 South Norfolk Council lawfully processes information about its residents, Members, employees, customers and other individuals in order to carry out its everyday business and to fulfil its public functions.

1.2 South Norfolk Council is committed to protecting the rights of privacy and processing will be conducted fairly, lawfully and transparently in accordance with relevant data protection legislation. Data Protection Legislation means the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) and any national implementing laws and secondary legislation, as amended or updated from time to time, in the UK, and any other successor legislation and all other applicable data protection law.

1.3 Data subjects have legal rights including the right to request: access to their data; rectification of an error; erasure of their details; restriction of processing; portability of their data; and to object to processing. To find out more about these rights please see Section 8.

1.4 This Policy must be read and complied with by all permanent staff, temporary staff, Councillors, Partner Organisations, other authorised third parties (suppliers and contractors) and all other authorised users. It must be adhered to when processing any of South Norfolk Council's personal data.

1.5 This policy is open to all internal and external stakeholders and is available on the Council's website www.south-norfolk.gov.uk

2. Responsibilities

2.1 Data Protection Legislation requires all public authorities to designate a Data Protection Officer. The Data Protection Officer for South Norfolk Council is involved in all matters which relate to the protection of personal data and is required to monitor compliance, provide advice and to cooperate/communicate with the Regulator as required.

2.2 The Senior Information Risk Owner (SIRO) is responsible for ensuring information assurance controls are in place.

2.3 The Strategic Leadership Team is responsible for developing and encouraging robust information handling practices within the Council.

2.4 Data protection champions have been nominated from across the Council who help to ensure that all the Council services maintain our high standards.

2.5 Beyond this, compliance with Data Protection Legislation is the responsibility of everyone that processes personal data on behalf of the Council. The Council, through its staff, Members and authorised third parties, is responsible for ensuring that any personal data is processed in accordance with Data Protection Legislation.

3. Data Protection Legislation Principles

3.1 All processing of personal data must be done in accordance with the data protection principles as prescribed in Data Protection Legislation:

a. Personal data shall be processed lawfully, fairly & transparently ('**lawfulness, fairness and transparency'**);

b. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation'**);
c. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation'**);
d. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy'**);
e. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('**storage limitation'**);
f. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality'**).

3.2 Furthermore, Data Controllers are required to be responsible for, and to demonstrate compliance with the principles ('**accountability'**).

The Council's accountability is demonstrated in numerous ways, including: the provision of mandatory data protection training, and refresher training; through the assignment of responsible individuals across the organisation (as set out at Section 2) including the assignment of the Data Protection Officer and Data Protection Champions from across the teams who help to maintain high standards of data privacy; and through the application of Council policies which are all regularly reviewed, promoted and accessible.

4. Lawful processing

4.1 Personal data will be lawfully processed by the Council at all times.
4.2 There are six ways in which lawful processing can occur, however only five of these are available to the Council as a public authority in the performance of tasks.
4.3 These five ways of lawful processing are:

a. The data subject **consents** to the processing for one or more specific purpose.
b In the performance of a **contract** to which the data subject is a party
c. In compliance with a **legal obligation**.
d. It is necessary to protect the **vital interests** of the data subject
e Processing is necessary for the performance of a task carried out in the public interest or in **the exercise of the official authority** vested in the controller.

4.3 When South Norfolk Council exercises its official obligation to provide services, the lawful ground generally used will be 4.2 (e). The Council hereby acknowledges the Regulator's Guidance on Consent which identifies that

public authorities will rarely be able to use consent as their lawful processing ground. However, where direct marketing is being carried out consent will ordinarily be required.

4.4 The Council will be clear and transparent in Privacy Notices, detailing the purposes for which we are collecting your data.

4.5 Wherever the lawful ground of processing is consent, consent will be requested:

4.5.1 In clear, specific and plain language.
4.5.2 Separate from other matters. If the processing is necessary for the provision of a service or the performance of a contract consent is unlikely to be a suitable lawful processing ground.
4.5.3 Able to put individuals in control of their data, build trust and engagement and maintain the Council's high-standards.
4.5.4 Important in providing genuine choice and control. It will be an affirmative action and will not be deemed or gathered by pre-ticked or opt-out boxes.
4.5.5 As easy to withdraw as it was to give consent. We will clearly explain how consent can be withdrawn and continue to do so in future interactions.
4.5.6 Reviewed and refreshed regularly.
4.5.7 Acted upon, ensuring that appropriate action is taken to prevent further processing where consent is withdrawn.

4.6 If any member or officer of the Council is in any doubt about these matters, they should contact the Data Protection Officer.

5. Privacy Notices

5.1 When we collect personal data from data subjects we will always provide clear information in a privacy notice. Data Protection Legislation stipulates the information which must be provided. South Norfolk Council's Privacy Policy provides further details.

6. Security of Data

6.1 The Council implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
6.2 All staff are responsible for ensuring that any Council personal data which they hold are kept securely and that they are not disclosed to any unauthorised third parties.
6.3 All personal data should be accessible only to those who need to use it. To ensure an appropriate level of security, we will keep personal data:

- In a locked room with access controlled; or
- In a locked drawer or filing cabinet; or
- If computerised, ensure data is only accessible to the required individuals; or

- Kept on encrypted disks, which are themselves stored securely.

6.4 Care should be taken to ensure that PCs and screens are not visible except to authorised individuals. Computer passwords must be kept confidential.

6.5 Care must be taken with the deletion or disposal of personal data ensuring safe disposal in line with the Records Management Policy. Physical records should be shredded or placed in the confidential blue wheeled bins.

6.6 Electronic records should be securely stored and deleted from Council systems in line with the Council's Retention Guidelines and Records Management Policy. The Council maintains a back-up system for use in emergencies in line with its IT Back-Up Policy.

6.7 Where data is transferred to a third-party individual or organisation, we take every step to ensure that this data is secure. We cannot however be held responsible for data once it reaches the third party unless that third party is an authorised data processor for the Council in which case we take due diligence to ensure they meet Council standards of security.

6.8 Where personal data is transferred to a third-party individual or organisation security measures will be taken to prevent a security breach in transit (these may include sending emails through a secure server or by password protecting that document).

6.9 The Council has measures in place to ensure compliance with security requirements which are regularly reviewed through internal audit reviews.

6.10 The Council is committed to ensuring that any breaches of data security are promptly reported to, and robustly investigated by, the Data Protection Officer so that mitigating steps can be taken at the earliest opportunity. Where legally required the Data Protection Officer will notify the Information Commissioner of any relevant breaches in line with our Breach Notification Procedure.

7. Rights of Data Subjects

7.1 Data Protection Legislation provides individuals with the rights to request:

a) access to their data;
b) portability of their data;
c) erasure of their data;
d) to object to processing;
e) to rectification of their data;
f) to restrict processing.

7.2 The rights set out at 7.1 are not absolute rights and may be dependent upon the lawful processing ground used. Furthermore, they may be subject to an exception or exemption as set out under Data Protection Legislation.

7.3 Where a data subject wishes to exercise one of these rights, they should contact the Data Protection Officer:

The Data Protection Officer
e) right2know@s-norfolk.gov.uk
t) 01508 533943

7.4 When we process a request to exercise one of your rights we will take reasonable authentication steps to verify your identity.

7..5 When one of the rights detailed at 7.1 are exercised, these will be actioned by the Council without undue delay and ordinarily within one month. This time may on occasion be extended by up to two months, in compliance with Data Protection Legislation. Where it is necessary to extend this time we will inform you of the reasons for this delay.

7.6 Subject Access Request

A subject access request made in electronic form will ordinarily be responded to in the same format, unless otherwise requested.

A charge will not ordinarily be made for a subject access request. Data Protection Legislation prescribes that a charge could only be made whereby further copies of personal data are requested by a data subject.

7.7 Portability

The right of portability only applies to processing carried out by automated means which is based on consent or on the performance of a contract.

If you have a right of portability where possible interoperable systems will be used to transfer your personal data, however where this is not technically possible the data will be transferred in an acceptable format.

7.8 Erasure

The right of erasure does not apply to processing which is subject to the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Whereby you have an applicable right of erasure we will let you know when we will be able to delete your details from our systems. This will be without undue delay, and within one month.

As a local authority we are required to have a robust back-up system and as such any applicable personal data will be deleted from our back-up systems after a period of 24 months.

7.9 Objection

Individuals can also object to personal data processed under grounds detailed at 4.3(e) or (f)

An objection to processing of personal data for direct marketing purposes cannot be refused.

Where an objection to processing is made and a relevant exception does not apply this Council will cease to process your personal data.

7.10 Rectification

Where inaccurate personal data is gathered you have the right to the rectification of this data. Rectification will occur without undue delay and ordinarily within one month.

7.11 Restriction

Where a right to restriction of processing applies such personal data shall, with the exception of storage, only be processed with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal persons or for reasons of public interest.

8. The Regulator – The Information Commissioner's Office

8.1 The Information Commissioner regulates the compliance of Data Protection Legislation across the UK. The Information Commissioner's details are:

Information Commissioner's Office,
Wycliffe House,
Water Lane, Wilmslow,
Cheshire, SK9 5AF
https://ico.org.uk/
(t) 0303 123 1113

8.2 The Council, as a Data Controller, is required to pay the Regulator a fee on an annual basis.

8.3 If you have any queries or concerns about how the Council process personal data you can contact the Council's Data Protection Officer.

8.4 You also have a right to lodge a complaint with the Information Commissioner's Office.

9 Disclosure of Data

9.1 Personal data may be lawfully disclosed where one of the following conditions apply:

- The individual has given their consent (eg. a member of staff or a customer has consented for the Council to correspond with a named third party).
- There is a Power of Attorney in place which authorises a third party to act on behalf of the data subject in relation to that issue.
- Where an exemption under Data Protection Legislation applies, including for the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment/collection of a tax or duty or an imposition of a similar nature.
- Where the authority is legally obliged to disclose data.

If in doubt, please consult the Council's Data Protection Officer.

10 Freedom of Information Act 2000

10.1 The Freedom of Information Act 2000 allows the public access, subject to certain exemptions, to all types of non-personal information held by public authorities, including this Council. However, requests for personal information will be dealt with under Data Protection Legislation.

11 Policy Review

11.1 This Policy will be reviewed every two years, and sooner if any issues are highlighted, in the case of new risks, and/or if there are changes in legislation.

12 Further Information

12.1 For further guidance or advice on the data protection legislation, please contact the Council's Data Protection Officer:
e) right2know@s-norfolk.gov.uk
t) 01508 533943.