Information & Data Protection Policy

1. Introduction

The Council recognises it must at times, keep and process sensitive and personal information about both employees and the public, it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards. This Policy is linked to the Quality Policy Statement, which will ensure information considerations are central to the ethos of the Council, and to the ICT Policy.

The Council will be very open about its operations and will work closely with public, community and voluntary organisations. Therefore in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Town's communities. Details of information which is available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

Information takes many forms and includes hard copy data printed or written on paper, data stored electronically, communications sent by post/courier or using electronic means, stored tape or video and speech.

2. About this Policy

The types of personal data that we may be required to handle include information about current, past and prospective suppliers, customers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act), the General Data Protection Regulation ((EU) 2016/679) (GDPR) and the Data Protection Bill 2017, and other regulations.

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of an employee's contract of employment and may be amended at any time.

This policy has been approved by the Council. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. That post is held by the Town Clerk, townclerk@sprowston-tc.gov.uk telephone 01603 408063. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the Data Protection Officer.

3. Definition of Data Protection Terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data or other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or can be an opinion about that person, their actions and behaviour.

Data Controller is the person who or organisation which determines the purposes of which, the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. Sprowston Town Councillors are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle data on the Council's behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. Making Information Available

The Publication Scheme is a means by which the Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. It is supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards, the website and sent to the local media. The Council publishes an annual programme in May each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation and has a public participation session on each Council and committee meeting. Details can be seen in the Council's Standing Orders, which are available on it's website or at its office.

Occasionally, Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Council are willing to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

5. Protecting Confidential or Sensitive Information

The Data Protection Act 1998 seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information. The policy is based on the principles below.

The Council will make any notification required to the Information Commissioner's Office under the Data Protection Act and periodically update the information.

6. Data Protection Principles

The Council and its employees will comply with the eight enforceable principles of good practice for processing sensitive data. These provide that personal data must be:

- Fairly & lawfully processed
- Processed for limited purposes and in an appropriate way
- Adequate, relevant & not excessive for the purpose
- Accurate and up to date
- Not kept longer than is necessary
- Processed in accordance with the data subject's rights
- Secure

- Not transferred to people or organisations situated in countries without adequate protection for the individual.

7. Fair and lawful processing

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

The Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any sensitive personal information and the Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual
- Required by law to process the data for employment purposes
- A requirement in order to protect the vital interests of the individual or another person

The Council will always give guidance on personnel data to employees through the Employee handbook.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

8. Disclosure Information

The Council will as necessary undertake checks on both staff and Members with the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure in its integrated quality management system.

9. Data Transparency

The Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This sets out the key principles

for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

Public data means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

The Code will therefore underpin the Council's decisions on the release of public data and ensure it is proactive in pursuing higher standards and responsible to best practice as it develops.

The principles of the Code are:

Demand led: new technologies and publication of data should support transparency and accountability

Open: the provision of public data will be integral to the Council's engagement with residents so that it drives accountability to them.

Timely: data will be published as soon as possible following production.

10. **Notifying data subjects**

If we collect personal data directly from data subjects, we will inform then about:

(a) the purpose or purposes for which we intend to process that personal data;
(b) the types of third parties, if any, with which we will share or to which we will disclose that personal data;
(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

We will inform data subjects whose personal data we process that we are the data controller with regard to that data and who the Data Protection Officer is.

11. **Adequate, relevant and non-excessive processing**

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

12. **Accurate data**

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

13. **Timely processing**

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our

systems, all data which is no longer required.

14. Processing in line with data subject's rights

We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller

(b) Prevent the processing of their data for direct-marketing purposes

(d) Ask to have inaccurate data amended

(e) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

15. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Council's central computer system instead of individual PCs.

Security procedures include:

Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

16. Transferring personal data to a country outside the European Economic Area (EEA)

We may transfer any personal data we hold to a country outside the European Economic

Area (”EEA”), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

17. Disclosure and sharing of personal information

We may disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

18. Dealing with subject access requests

Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Data Protection Officer immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Our employees will refer a request to the Town Clerk for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

19. **Changes to this Policy**

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

SCHEDULE 1
Data Processing Activities

Type of data	Type of data subject	Type of processing	Purpose of processing	Type of recipient to whom personal data is transferred	Retention period

- In the course of our business, we may collect and process the personal data set out in the *Schedule 1*. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

- We will only process personal data for the specific purposes set out in the *Schedule 1* or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

- We may also share personal data we hold with selected third parties for the purposes set out in the *Schedule 1*.