DATA PROTECTION POLICY

CONTENTS

1. POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of the Town Council's activities, it will collect, store and process personal information about its staff, Councillors and electorate, and it recognises the need to treat it in an appropriate and lawful manner.

1.2 The types of information that the Town Council may be required to handle include details of current, past and prospective employees, suppliers and customers, in accordance with our document retention policy. The information which may be held on paper or on a computer or other media is subject to certain legal safeguards specified in the UK Data Protection Act 2018 (the Act) and General Data Protection Regulation 2018. The Act imposes restrictions on how it may use that information.

1.3 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously any may result in disciplinary action.

2. STATUS OF THE POLICY

2.1 This policy sets out the Town Council's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 If you consider that the policy has not been followed in respect of personal data about yourself or other you should raise the matter with the Chair of the Finance and Governance Committee.

3. DEFINITION OF DATA PROTECTION TERMS

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

3.2 **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 data.

3.3 **Personal Data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 **Data Controller** is the Proper Officer of Lowestoft Town Council and its Councillors, who determines the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. They are the data controller of all personal data used in our business.

3.5 **Data Users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 **Data Processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers who handle personal data on our behalf.

3.7 **Data Protection Officer** is responsible for all data protection procedures and policies and subject access requests.

3.8 **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.

3.9 **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 accessed under strict conditions, and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These stipulate that personal data must be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant and not excessive for the purpose
- Accurate
- Not kept longer than necessary for the purpose
- Processed in line with data subjects' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is intended not 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. The data subject must be told who the data controller is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6. PROCESSING FOR LIMITED PURPOSES

6.1 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

8. ACCURATE DATA

8.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. TIMELY PROCESSING

9.1 Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from the Town Council's systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Clerk.

10. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

10.1 Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data about them by a data controller
- Prevent the processing of their data for direct-marketing purposes

- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to themselves or anyone else

11. DATA SECURITY

11.1 The Town Council must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The Act requires us to 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 may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate security measures themselves.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only the Proper Officer is authorised to use the data and 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

11.4 Security procedures include:

- Data stored on computers should be protected by strong passwords that are changed regularly
- 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.
- Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by
- All servers containing sensitive data must be approved and protected by security software and a strong firewall

12. SUBJECT ACCESS REQUESTS

12.1 Under the UK Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them. Any subject access request received will be immediately referred to the Data Protection Officer, who may ask officers and Councillors to help comply with those requests. Please contact the Town Council if you

would like to correct or request information that Council holds about you. There are also restrictions on the information to which an individual is entitled under applicable law.

13. PROVIDING INFORMATION OVER THE TELEPHONE

13.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the Town Council. They should ask the caller to put their request in writing and refer to the Clerk for assistance in difficult situations. No one should be bullied into disclosing personal information.

14. GDPR AND DATA PROTECTION ACT PROVISIONS

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

14.1 **Privacy Notice – transparency of data protection**

Being transparent and providing accessible information to individuals about how the Council will use individuals' personal data is important for our organisation.

14.2 **Conditions for Processing**

The Council will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented.

14.3 **Justification for Personal Data**

The Council will process personal data in compliance with the following six data protection principles:

- Personal data is processed lawfully, fairly and in a transparent manner
- Personal data is collected only for specified, explicit and legitimate purposes
- Personal data is processed only where adequate, relevant and limited to what is necessary for the purposes of processing
- Personal data is kept accurate and all reasonable steps are taken to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data is kept only for the period necessary for processing
- Appropriate measures are adopted to ensure that personal data is secure and protected against unauthorised or unlawful processing and accidental loss, destruction or damage

The Council will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

14.4 **Consent**

The data that the Council collects is subject to active consent by the data subject. This consent can be revoked at any time.

14.5 **Criminal Record Checks**

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

14.6 **Data Portability**

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

14.7 **Right to be Forgotten**

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

14.8 **Privacy by Design and Default**

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan. When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

14.9 **Data Audit and Register**

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

14.10 **Reporting Breaches**

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Council to:

- Investigate the failure and take remedial steps if necessary
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures with 72 hours of discovery
- To report a breach, please contact the Data Protection Officer via sarah.foote@lowestofttowncouncil.gov.uk

14.11 **Monitoring**

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

14.12 **Consequences of Failing to Comply**

Compliance with this policy is taken very seriously. Failure to comply puts both the individual (Councillor or Officer) and the Council at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under the Council's procedures which may result in dismissal.