KESSINGLAND PARISH COUNCIL

DATA PROTECTION POLICY

ADOPTED: 21 MAY 2018

TO BE REVIEWED ANNUALLY

CONTENTS

1. Policy Statement 1

2. Status of the Policy 1

3. Scope of the Policy 1

4. Definition of Data Protection Terms 2

5. Purposes for which Personal Data may be used by us 2-3

6. Fair and Lawful Processing 3-6

7. Subject Access Request 6

8. Processing Data in Accordance with Individual's Rights 6

9. Training 7

10. GDPR Provisons 7-8

11. Reporting Breaches 8-9

12. Monitoring 9

13. Consequences of Failure to Comply 9

1. POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities, we will collect, store and process personal information about our residents, staff and other third parties, and we recognise the need to treat it in an appropriate and lawful manner in accordance with General Data Protection Regulations that come into force on 25 May 2018.

1.2 This policy sets out how we seek to protect personal data and ensure that Councillors and Officers understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires Officers to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.3 The types of information that we may be required to handle include details of residents, the public, current, past and prospective employees, suppliers, customers and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulations and other legislation. The Regulations imposes restrictions on how we may use that information.

1.4 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 and may result in disciplinary action.

2. STATUS OF THE POLICY

2.1 This policy sets out our 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 others you should raise the matter with the Data Protection Officer.

3. SCOPE OF THE POLICY

3.1 This policy applies to all councillors and staff. You must be familiar with this policy and comply with its terms.

3.2 This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3.3 Who is responsible for this policy?

As our Data Protection Officer, the Clerk, has overall responsibility for the day-to-day implementation of this policy.

4. DEFINITION OF DATA PROTECTION TERMS

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

4.2 **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.

4.3 **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).

4.4 **Data controllers** are the people who or organisations which determine 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. We are the data controller of all personal data used in our business.

4.5 **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.

4.6 **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 which handle personal data on our behalf.

4.7 **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.

4.8 **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. Under the new regulations, it also includes genetic data, biometric data, and sexual orientation. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

5. PURPOSES FOR WHICH PERSONAL DATA MAY BE USED BY US

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes.

	Council purposes include the following: - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring Council policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Promoting Council services* - *Improving services*

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts, members of the public, Council service users, residents, market traders, hirers, correspondents *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails, databases, council records*
Sensitive personal data	*Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.*

6. FAIR AND LAWFUL PROCESSING

6.1 We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

6.2 **The Data Protection Officer's Responsibilities:**

- Keeping the Council updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis

- Assisting with data protection training and advice for all staff members and those included in this policy

- Answering questions on data protection from staff, council members and other stakeholders

- Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them by Kessingland Parish Council.

- Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing.

6.3 **Responsibilities of the Parish Clerk**

- Ensure all systems, services, software and equipment meet acceptable security standards.

- Checking and scanning security hardware and software regularly to ensure it is functioning properly.

- Researching third-party services, such as cloud services the company is considering using to store or process data.

- Approving data protection statements attached to emails and other marketing copy.

- Addressing data protection queries from clients, target audiences or media outlets

- Co-ordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

6.4 **The processing of all data must be:**

- Necessary to deliver our services

- In our legitimate interests and not unduly prejudice the individual's privacy

- In most cases this provision will apply to routine business data processing activities.

6.5 Our Terms of Business contains a Privacy Notice relating on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers, employees, residents and service users.

- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers or pass information to other public sector bodies in relation to resident complaints / queries.

- Provides that service users and correspondents have a right of access to the personal data that we hold about them

6.6 **Sensitive Personal Data**

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

6.7 **Accuracy and relevance**

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, Donna Lee.

6.8 **Your Personal Data**

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

6.9 **Data Security**

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

6.10 **Storing Data Securely**

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it

- Printed data should be shredded when it is no longer needed

- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.

- Data stored on CDs or memory sticks must be locked away securely when they are not being used

- The DPO must approve any cloud used to store data

- Servers containing personal data must be kept in a secure location, away from general office space

- Data should be regularly backed up in line with the council's backup procedures

- All servers containing sensitive data must be approved and protected by security software and strong firewall.

6.11 **Data Retention**

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

7. SUBJECT ACCESS REQUESTS

7.1 Please note that under GDPR individuals are entitled, subject to certain exceptions, to request access to information held about them.

7.2 If you receive a subject access request, you should refer that request immediately to the DPO. Who may ask you to help us comply with those requests.

7.3 Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

8. PROCESSING DATA IN ACCORDANCE WITH THE INDIVIDUAL'S RIGHTS

8.1 You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

8.2 Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

8.3 Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

9. TRAINING

9.1 All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis. It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

10. GDPR PROVISIONS

The following provisions will take effect from 25 May 2018.

(a) Privacy Notice - Transparency of Data Protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?
Who is collecting it?
How is it collected?
Why is it being collected?
How will it be used?
Who will it be shared with?
Identity and contact details of any data controllers
Retention period

(b) Conditions for Processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

(c) Justification for Personal Data

We will process personal data in compliance with all six data protection principles.

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

(d) Consent

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

(e) **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.

(f) **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.

(g) **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.

(h) **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.

(i) **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.

11. REPORTING BREACHES

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

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Compliance Failure Policy for our reporting procedure.

12. 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.
Councillors should ensure that they deal with all council business via their council email address and not via their personal ones. It is preferable that council employees and councillors access their email addresses via their council provided laptop, but should they add their council email address to their own personal devices it is their responsibility to adhere to the rules and regulations as set out within this policy and should they leave the council all council related documentation stored on this device is deleted with immediate effect.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.

A Councillor could be found in breach of the Suffolk Code of Conduct.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.