Kersey Parish Council Data Protection and Information Security Policy

Introduction

Kersey Parish Council has a responsibility under the Data Protection Act 2018 and other regulations to hold, obtain, record, process, store and destruct all personal data relating to an identifiable individual in a secure, appropriate and lawful manner. Data may be held in paper or electronic form.

Kersey Parish 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 sets out the Parish Council's rules on data protection and the legal conditions that must be satisfied in relation to personal data. This policy applies to all Parish Council employees, councillors, volunteers and contractors.

The Parish Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Parish Council is the data controller. The Clerk as Proper Officer of the Parish Council is the data protection lead for Kersey Parish Council.

Data Protection Terminology

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

Data Subject - means the person whose personal data is being processed. This includes all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal data.

Personal Data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person. It can be anything from a name, a photo, and an address, date of birth, an email address or it can be an opinion such as a performance appraisal.

Sensitive Personal Data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data Controller - means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is to be processed.

Data Processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. This could include contractors which handle personal data on our behalf.

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

Data Protection Principles

The Parish Council fully endorses and adheres to the data protection principles as set out in the Act. All data covered by the Act must be handled in accordance with the Six Data Protection Principles:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Processed for limited, legitimate purposes and in an appropriate way.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.

- Not kept longer than necessary for the purpose.
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Processing in Line with Data Subject's Rights

Data must be processed in line with data subjects' rights. The Parish Council must ensure individuals can exercise their rights in the following ways:

- Right to be informed
  - providing privacy notices
  - keeping a record of how the Parish Council uses personal data to demonstrate compliance
- Right of access:
  - enabling individuals to access their personal data and supplementary information
  - allowing individuals to be aware of and verify the lawfulness of the processing activities
- Right to rectification:
  - rectifying or amending personal data of the individual if requested
  - carrying out the above process within one month
- Right to erasure:
  - deleting or removing an individual's data if requested and there is no compelling reason for its continued processing
- Right to restrict processing:
  - complying with any request to restrict, block or supress the processing of personal data
  - retaining only enough data to ensure the right to restriction is respected in the future
- Right to data portability:
  - providing individuals with their data so that they can reuse it for their own purposes
  - providing it in a commonly used format (i.e. machine-readable format)
- Right to withdraw consent
  - respecting the right of an individual to withdraw consent to the processing at any time for any processing of data to which consent was obtained
  - withdrawal can be by telephone, email or by post
- The right to lodge a complaint with the Information Commissioner's Office.
  - contacting the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Roles and Responsibilities

The Clerk and Councillors will ensure that:

- Personal information is treated in a confidential manner in accordance with this and any associated policies.
- The rights of data subjects are respected at all times.
- Privacy notices will be made available to inform individuals how their data is being processed.
- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose.
- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information.
- Personal information is recorded accurately and is kept up to date.

- They appropriately handle any subject access requests and/or requests in relation to the rights of individuals.
- They appropriately handle actual or potential breaches of the Data Protection Act as soon as the breach is discovered.
- It is the responsibility of the Clerk and Councillors to ensure that they comply with the requirements of this policy and any associated policies or procedures.

Contractors

Where contractors are used, the contracts between the Parish Council and these third parties should contain mandatory information assurance clauses to ensure that the contract staff are bound by the same rules, as listed above for the Clerk and Parish Councillors in relation to the Data Protection Act.

Volunteers

All volunteers are bound by the same rules, as listed above for the Clerk and Parish Councillors in relation to the Data Protection Act.

Data Security

The Parish Council will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

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 measures.

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

- Confidentiality means that access to data is limited to the Proper Officer or other authorised persons for whom access is necessary in the course of their work.
- 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.

Security procedures include:

- Secure lockable drawers and/or cupboards. Drawers and cupboards should be kept locked if they hold confidential information of any kind.
- All computers used to access or process Parish Council personal data eg. e-mails must have virus protection and a firewall.
- Password protection is used.
- Methods of disposal. Paper documents should be shredded or burnt. Electronic data will be deleted.

The Parish Council will ensure that information is not transferred to countries outside the European Economic Area (EEA) unless that country has an adequate level of protection for security and confidentiality of information which has been confirmed by the Information Commissioner.

Kersey Parish Council Data Protection and Information Security Policy

Records Management and Data Audit

Good records management plays a pivotal role in ensuring that the Parish Council is able to meet its obligations to provide information, and to retain it, in a timely and effective manner in order to meet the requirements of the Act. The Parish Council has carried out a data audit which will be regularly updated. All records should be retained and disposed of in accordance with the Parish Council Data Retention Policy.

Data Protection Impact Assessments

Data protection impact assessments will be carried out where appropriate as part of the design and planning of projects, systems and programmes.

Data Breaches

Under the GDPR, the Parish Council is required to report a personal data breach, which meets the reporting criteria, to the Information Commissioner within 72 hours of the Council becoming aware of the breach. Guidance states that organisations should notify the Information Commissioners Office of a breach where it is likely to result in a risk to the rights and freedoms of individuals or if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

In the event of a data breach the Proper Officer will immediately inform the Chair of the Parish Council. They will then take all the necessary measures to manage the breach.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Parish Council will notify those individuals concerned directly.

In line with the accountability requirements, all data breaches must be recorded by the Parish Council along with details of actions taken. This record will help to identify system failures and should be used to improve the security of personal data.

Dealing with Subject Access Requests (SAR)

Individuals wishing to request their information as a subject access request should contact the Parish Council, who will arrange for the information to be processed in accordance with the Data Protection Act and Kersey Parish Council's Subject Access Request Policy.

Access to Policies Referred to Under this Policy

For details of all policies relevant to Kersey Parish Council as a local government authority please visit the Parish Council's website www.kersey.suffolk.gov.uk

The Parish Council will periodically review and revise this policy in the light of experience, comments from data subjects and guidance from the Information Commissioners Office.

Data Protection and Information Security Policy adopted on: 10 September 2018 Minute ref: 126/18