Candovers Parish Council

Data Protection (General Data Protection Regulations [GDPR]) Policy)

Introduction

Candovers Prish Council needs to hold certain information about individuals for a variety of business purposes.

This policy states how personal data will be collected, handled and stored to meet data protection standards and to ensure employees understand the rules governing the use of personal data to which they have access in the course of their duties.

This policy ensures Candovers Parish Council:

- Complies with the Data Protection Act 2018 and UK General Data Protection Regulations (GDPR) and follows good practice.
- Protects the rights of the employees and all other stakeholders.
- Is open about how it stores and processes an individual's data.
- Protects itself from the risk of data breach.
- Is committed to conducting its business in accordance with all applicable data protection laws and regulations and is in line with the highest standards of ethical conduct.

Applicability

This policy applies to the processing of personal data for customers, employees (current or former), suppliers, business contacts, candidates for jobs and other stakeholders in manual and electronic records kept by Candovers Parish Council in connection with its business. It also covers Candovers Parish Council's response to any data breach and other rights under UK GDPR.

This policy applies to all company employees who process personal data while carrying out their business activities.

Key terms

'*Personal data*' is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, or online identifier. It can also include pseudonymised data. Candovers Parish Council uses the personal data of its contacts for the following purposes: the general running and business administration and to provide services to its customers.

'*Sensitive personal data*' is data that relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion or trade union membership. It also includes genetic and biometric data used for ID purposes.

'*Criminal offence data'* is data that relates to an individual's criminal history.

'*Data processing'* is any operation or set of operations that are performed on personal data or on sets of personal data. This may be by automated means such as collection, recording, organisation structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'*Data subject*' is the individual to whom the personal data relates.

The '*Data Protection Officer'* (DPO) informs and advises on obligations to comply with UK GDPR and other data protection legislation and monitors compliance. This includes managing internal data protection activities, advises on data protection impact assessments, trains staff and conducts internal audits. They are the first point of contact for supervisory authorities such as the Information Commissioner's Office, individuals whose data is processed, business development purposes, personnel, administrative, financial, regulatory and payroll.

Candovers Parish Council makes a commitment to ensuring that personal data, including sensitive personal data and that relating to criminal offence data, is processed in line with UK GDPR and domestic law. All its employees conduct themselves in line with this and other related policies. Where Candovers Parish Council uses third parties to process data on its behalf, Candovers Parish Council will ensure that the third party takes such measures to maintain Candovers Parish Council's commitment to protecting data. Candovers Parish Council understands that it will be accountable for the processing, management, regulation, storage and retention of personal data held electronically and in the form of manual records.

Types of data held

Data is likely to comprise:

- Name, address, email address, telephone number and other contact information.
- Next of kin details.
- Bank details and National Insurance number.
- Right to work in the UK documentation and other security screening information.
- Driving licence or Passport.
- Medical information.
- Absence, disciplinary and grievance records.
- Qualifications, skills, experience and employment history.
- Current level of renumeration, including benefit entitlement.
- Disability.
- Contracts with clients and suppliers.
- Email traffic.
- Web browsing activity

- CCTV recording on company property
- Mailing lists

Individuals should refer to Candovers Parish Council's privacy notices for more information on the reasons for its processing activities and the lawful basis it relies on for the processing and data retention periods.

Data protection principles

When dealing with personal data Candovers Parish Council shall ensure that the following seven principles are adhered to:

1. Fair Lawful and Transparent Processing
   All personal data will be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. Purpose limitation
   It will be clearly specified exactly what the personal data to be collected will be used for and limit the processing of the data to only that which is necessary to meet the explicit, legitimate and specified purpose.

3. Data minimisation
   Personal data will be adequate, relevant and limited to that which is necessary in relation to the purposes for which it is processed, personal data beyond that which is strictly required will not be stored.

4. Accuracy and relevance
   Any personal data processed will be accurate and relevant, not excessive and kept up to date. Inaccurate data will be erased or rectified without delay.

   The measures adopted by Candovers Parish Council to ensure data quality include:

   - Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request it.
   - Keeping personal data only for the period necessary to satisfy the permitted uses or applicable retention period.
   - The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
   - Restriction rather than deletion of personal data in so far as the law prohibits erasure.
   - Erasure would impair the legitimate interests of the data subject.

5. Storage limitation, data retention and storing data securely

Wherever possible, personal data will be stored in a way that limits or prevents identification of the data subject. All personal data will be deleted or destroyed as soon as possible where it has been confirmed there is no longer a need to retain it.

- Where data is stored on printed paper it will be kept in a secure place where unauthorised persons cannot access it.
- Printed data will be shredded and placed in confidential waste bags when it is no longer required.
- Data stored electronically will be protected by strong passwords that are changed regularly. All staff will be encouraged to use a password manager to create and store passwords.
- [The DPO must approve any 'cloud' used to store data].
- Servers containing personal data will be kept at a secure location away from general office space.
- All servers containing sensitive data will be protected by security software and strong firewalls.
- Data will be regularly backed up in line with the backup procedures
- Data will never be saved directly to mobile devices such as laptops, tablets or smartphones.

6. Integrity, confidentiality and data security.
   Personal data will be processed in a manner that ensures appropriate security of the data including protection against unauthorised or unlawful processing, against accidental loss, destruction or damage using appropriate technical or organisational measures.

7. Accountability
   The Data Controller shall be responsible for and be able to demonstrate compliance with UK GDPR and review and update relevant policies and procedures.

Individual's rights.

Personal data will be processed in recognition of an individual's data protection rights as follows:

- The right to be informed.
- The right of access.
- The right for any inaccuracies to be corrected.
- The right to have information deleted.
- The right to restrict the processing of the data.
- The right of portability.
- The right to object to the inclusion of any information.
- The right to regulate any automated decision-making and profiling of personal data.

Employees personal data.

Employees must take responsible steps to ensure that the personal data held about them is accurate and updated as required. This would include changing a name or address.

Children's personal data.

[Children's data is not processed by Candovers Parish Council].

Privacy notices

Privacy notices are issued to all individuals whose personal data is possessed by Candovers Parish Council.

These notices set out the purpose for which it holds the data, what data is collected, who it is shared with, how it is stored, how long it is retained and the individual's data protection rights.

Candovers Parish Council's website includes an outline privacy notice and an online cookie notice fulfilling the requirements of applicable law.

Access to data

Individuals are entitled to request access to information held about them. Candovers Parish Council will consider each request in accordance with all applicable data protection laws and regulations.

- Subject access requests should be made in writing and submitted to the Chairman of the Parish Council and sent either by post to:

  3 Farriers Close, Preston Candover, Hampshire, RG25 2EZ

  or via email to: clerk@candoversparishcouncil.com

- Candovers Parish Council will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive. Information will not be passed to third parties even at the request of the applicant.
- Candovers Parish Council will respond to a request without delay. Access to data will be provided subject to legally permitted exemptions within a maximum of one month. This may be extended by a further two months if requests are complex or numerous.
- If a request is refused, individuals must be advised why this is so within a month of the request being received.
- Individuals must inform the Chairman of the Parish Council immediately if they believe the data is inaccurate, either because of a subject access request or otherwise. The Chairman of the Parish Council will take immediate steps to rectify the information.

Data disclosures and transfers.

Candovers Parish Council may disclose or transfer personal data to internal or third-party recipients. The circumstances leading to such a disclosure include sending information to:

- Other third parties who provide services to the Council, i.e. pensions providers or a payroll provider.
- Where there is a legal obligation to do so, for example, where there is a requirement to share information under statute to prevent fraud and other criminal offences. This may be in the form of a court order from the police or HMRC.

These kinds of disclosures and transfers will only be made when strictly necessary.

Candovers Parish Council does not transfer personal data outside of the European Economic Area (EEA).

Data security

Candovers Parish Council will adopt physical, technical and organisational measures to ensure the security of personal data when it is stored and transported. This includes the prevention of loss or damage, unauthorised alteration, access or processing and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the personal data related security measures in place is provided below:

- Prevent unauthorised persons from gaining access to data processing systems.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisation.
- Ensure that personal data, in the course of electronic transmission during transport, cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether and by whom, the personal data was entered, modified or removed from a data processing system.
- Ensure that in the case where processing is conducted by a data processor, the data can be processed only in accordance with the instructions of the data controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary.

In addition, employees must:

- Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- Ensure that all files or written information of a confidential nature are not left where unauthorised people can read them.

- Check regularly on the accuracy of data being entered into computers.
- Always use secure passwords to access the computer systems and not abuse them by passing on to unauthorised persons.
- Lock the computer when not in use so that personal data is not left on screen when unattended.
- No personal email accounts should be used for council business.

Personal data relating to employees should not be kept or transported on laptops, USB sticks or similar devices unless authorised. Where any personal data is recorded on any device, it should be safeguarded in the following way:

- Ensuring that data is recorded only on the device if strictly necessary.
- Using an encrypted system – a folder should be created to store the files that need extra protection, and all files created or moved to this folder should be automatically encrypted.
- Ensuring that laptops or USB drives are kept securely to minimise theft.

Reporting a suspected data breach.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data.

All staff have an obligation to report actual or potential data protection compliance failures to the Chairman of the Parish Council. Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of Candovers Parish Council becoming aware of the breach. It may be reported in more than one instalment.

Individuals will be informed directly if a breach is likely to result in a high-risk to the rights and freedoms of that individual.

If the breach is significant enough to warrant notification to the public, Candovers Parish Council will do so without undue delay.

Procedures

Candovers Parish Council has taken the following steps to protect the personal data it holds or to which it has access to and appoints employees with specific responsibilities for:

- The processing and controlling of data.
- The comprehensive reviewing and auditing of its data protection systems and procedures.
- Overseeing the effectiveness and integrity of all the data that must be protected.

There are clear lines of responsibility and accountability for these distinct roles.

Furthermore Candovers Parish Council will:

- Provide information to its employees on their data protection rights, how it uses their personal data and how it protects it. The information includes the actions individuals can take if they think that their data has been compromised in any way.
- Provides its employees with information and training to make them aware of the importance of protecting personal data teaching them how to do this and understand how to treat information confidentiality.
- Account for all personal data it holds, where it comes from and with whom it is shared or likely to be shared.
- Conduct risk assessments as part of its reviewing activities to identify any vulnerabilities in the handling and processing of personal data, taking measures to reduce mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both.
- Recognise the importance of seeking individual's consent for obtaining, recording, using, sharing, storing and retaining their personal data, regularly reviewing procedures. Audit trails are needed and are followed for all consent decisions that must be freely given by an individual and should be specific, informed and unambiguous. Full information will be given regarding the activities about which consent is sought. Individuals have the absolute right to withdraw that consent at any time.
- Have appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches including security breaches. It is aware of the duty to report high-risk breaches that may cause significant harm to the affected individual to the Information Commissioner and is aware of the possible consequences.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take on discovering a potential data breach.

The nominated data controller/auditors/protection officers for Candovers Parish Council are trained appropriately in their roles under UK GDPR.

All employees who need to use the IT system are trained to protect the individuals' personal data, ensuring data security and to understand the potential consequences to themselves and Candovers Parish Council of lapses and breaches of policy and procedure in accordance with Candovers Parish Council's IT policy.

Records

Candovers Parish Council keeps records of its processing activities including the purpose for processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

Data Protection Officer (DPO)

Candovers Parish Council's DPO can be contacted via:
clerk@candoversparishcouncil.com