HORSMONDEN PARISH COUNCIL

Data Protection Policy

Horsmonden Parish Council, Parish Office, Horsmonden Village Hall, Back Lane, Horsmonden, Kent, TN12 8LH

Clerk: Mrs L. Noakes

Introduction

We hold personal data about our employees, residents, suppliers and other individuals for a variety of Council purposes.

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.

Definitions

Business purposes

The purposes for which personal data may be used by us:

- Personnel, administration, financial, statutory and legislative purposes, payroll, consultations and business development purposes.
- The 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 an 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 or condition, criminal offences, or related proceedings – any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

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

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.

Who is responsible for this policy?

As our Data Protection Officer, Richard Newell, GDPR-Info Ltd (who can be contacted via the Clerk to Horsmonden Parish Council: clerk@horsmonden-pc.gov.uk or telephone 01892 724989) has overall responsibility for the day-to-day implementation of this policy.

Our procedures

Fair and lawful processing

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.

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 Horsmonden Parish Council
- Checking and approving with third parties that handle the Council's data any contracts or agreements regarding data processing.

IT Responsibilities dealt with by the 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 Council is considering using to store or process data

Responsibilities of the Officers

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and other Council's Data Protection Policy

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interest and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice relation to 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
- Provides that service users and correspondents have a right of access to the personal data that we hold about them

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 processes and to whom it will be disclosed.

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, Jayne Cole, Chief Executive of Local Council Public Advisory Service.

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 information the Clerk to the Council, Mrs L. Noakes, so that she can update your records.

Data security

We will 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.

Storing data security

- 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

- 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/safe 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
- Data which is saved directly to mobile devices such as laptops, tablets or smartphones must be suitably protected with passwords, encryption or pin numbers.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

Personal data will be retained 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.

Subject Access Requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

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.

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.

Processing data in accordance with the individual's rights

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.

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.

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

Training

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 will cover:

- The law relating to data protection
- The Parish Council's related policies and procedures.

Completion of training is compulsory.

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.

Privacy Notice – transparency of data protection

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

What information is being collected?

1. Who is collecting it? Horsmonden Parish Council
2. How is it collected: By email, in writing, by telephone
3. Why is it being collected? To fulfil the Council's statutory functions and services or as a statutory requirement or consent
4. How will it be used? In association with providing the Council's statutory functions and services or its statutory requirements
5. Who will it be shared with? Members of Horsmonden Parish Council and its related bodies which are the Emergency Planning Group and Neighbourhood Planning Group. Third parties such as HMRC in association with carrying out the Council's functions as an employee. Your personal information will not eb shared with any third party without your prior consent.
6. Identity and contact details of any data controllers: Horsmonden Parish Council staff members: Lucy Noakes (Clerk) clerk@horsmonden-pc.gov.uk and Jackie Stanton (Assistant Clerk) assistantclerk@horsmonden-pc.gov.uk. Telephone: 01892 724989 or 07484 904765.
7. Retention period? We will only keep your data for the purpose it was collected for and only for as long as is necessary, after which it will be deleted or shredded.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing. 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.

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.

Consent

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

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.

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.

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.

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.

Data audit and register

Regular data audits to manage and mitigate risks will form 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.

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.

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.

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.

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