Hamsey Parish Council Data Protection Policy

1. Introduction

In order to adhere to the Data Protection Act 2018 and the General Data Protection Regulations Hamsey Parish Council has adopted the following policy.

Hamsey Parish Council holds personal data about employees, councillors, residents, suppliers, and other individuals for a variety of council purposes.

This policy sets out how the council seek to protect personal data and ensure that councillors and officers understand the rules governing the use of personal data to which they have access in the course of their work. This policy requires officers to ensure that the council be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed

This policy applies to all councillors and staff. The Clerk has overall responsibility for the day-to-day implementation of this policy.

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

2. The Clerk'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

• Answering questions on data protection from staff, council members and other Stakeholders

• Responding to individuals who wish to know which data is being held on them by Hamsey Parish Council.

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

• 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

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

• Coordinating with the council to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

• Privacy by design is an approach to projects that promotes privacy and data protection

compliance from the start. The Clerk will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan. This will be conducted by preparing an action plan at all stages of development, implementation and operation for each parish council project identifying the complete description in which the environment, application or capabilities where privacy and data protection requirements are applicable, identifying the systems and processes involved and addressing the risks throughout the lifecycle of the project.

3. The Council's responsibilities

• The council's website displays a Privacy Notice relating to data protection.

• In most cases where the council process sensitive personal data the council will require the data subject's explicit consent to do this unless exceptional circumstances apply, or the council 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

• The council will ensure that any personal data the council process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. The council 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.

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

4. Councillors and staff individual responsibilities

• Councillors and staff must take reasonable steps to ensure that personal data the council hold about subjects is accurate and updated as required.

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

• In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised persons 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. The council 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 council must approve any cloud used to store data by councillors or staff.

• Firewall software that comes with any network access device should be set to high security mode and any personal data stored in hard copy format should be stored in a secure location.

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

• Data should never be saved directly to mobile devices such as laptops, tablets or smartphones which can be used providing the item is Password protected, the network equipment used to download the emails has a firewall activated. Once the data has been used and is no longer required it is deleted from the user's systems, either on the machine or cloud storage device.

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

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

• Do not forward on emails or email threads that may contain personal data.

• Where possible direct all correspondence to the Clerk who can obtain the necessary consent.

• Inform the Clerk of any data breaches withing 48 hours

• Councillors will complete the GDPR checklist for Councillors, to confirm actions.

5. Subject Access

• 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 Clerk. Who may ask you to help the council comply with those requests.

• Please contact the Clerk if you would like to correct or request information that the council hold about you. There are also restrictions on the information to which you are entitled under applicable law.

6. 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

• 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

7. 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.

8. 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 the use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

9. Processing data in accordance with the individual's rights

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

Direct marketing material must not be sent to someone electronically (e.g. via email) unless the council has an existing business relationship with them in relation to the services being marketed.

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

10. 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. Monitoring
All councillors and staff must observe this policy.

The Clerk will monitor the implementation of the policy regularly to make sure it is being adhered to.

12. Information Commissioner's Office (ICO)

The Council is registered with the Information Commissioner's Office and pays the annual data protection fee as required.

ICO contact details:

Reference: ZB488252
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
www.ico.org.uk