LOCAL COUNCIL PUBLIC ADVISORY SERVICE

Gamlingay Parish Council

Information Protection Policy

Adopted: 09/10/2018

Reviewed: May 2019 (Appendix 1 added)

Contents

Document Control

Organisation	
Title	
Creator	
Source	
Approvals	
Distribution	
Filename	
Owner	
Subject	
Protective Marking	
Review date	

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description

1 Purpose

1.1 Information is a major asset that Gamlingay Parish Council has a duty and responsibility to protect.

1.2 The purpose and objective of this Information Protection Policy is to specify the means of information handling and transfer within the Council.

2 Scope

2.1 The Information Protection Policy applies to all Councillors, Committees, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Gamlingay Parish Council purposes.

2.2 Information takes many forms and includes:

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post / courier or using electronic means
- stored tape or video
- speech

3 Information Storage

3.1 All electronic information will be stored on centralised facilities to allow regular backups to take place.

3.2 Information will not be held that breaches the Data Protection Act (1998) or formal notification and guidance issued by Gamlingay Parish Council. All personal identifiable information will be used in accordance with the Caldicott Principles.

3.3 Records management and retention policy will be followed.

3.4 Staff should not be allowed to access information until line managers are satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

3.5 Databases holding personal information will have a defined security and system management policy for the records and documentation.

3.6 This documentation will include a clear statement as to the use, or planned use of the personal information, which is cross-referenced to the Data Protection Notification.

3.7 Files which are listed by Gamlingay Parish Council as a potential security risk should not be stored on the network, except for in designated application storage areas. To facilitate this Gamlingay Parish Council will implement an electronic File security solution.

4

Disclosure of Information - Computer and Paper Based

4.1 The disclosure of personal information to other than authorised personnel is forbidden. If there is suspicion of a Member or employee treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is be reported to the Data Control Officer (Clerk) who will take appropriate action.

4.2 Do not remove printed information from premises without the express consent of the information owner. Consent will only be given in exceptional circumstances

4.3 Protectively marked, personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.

4.4 Disposal methods for waste computer printed output and other media must be in accordance with Gamlingay Parish Councils disposal policy.

4.5 Distribution of information should be via the most secure method available.

5 Disclosure of Information – Telephone, Fax and E-mail

5.1 Where this involves the exchange of sensitive information then the following procedures will be applied.

6 Telephone calls:

6.1 Verify the identification of members before disclosing information. If in doubt, return their call using a known telephone number.

6.2 For external callers, verify their identity and their need to know the requested information. Telephone them back before releasing information and ask the caller to provide evidence of their identity (this could be passport, driving license, household bill).

6.3 Ensure that you are authorised to disclose the information requested.

6.4 Ensure that the person is entitled to be given this information.

6.5 Ensure that the information you give is accurate and factual.

7 Fax transmissions:

7.1 Fax should not be used to transmit personal or sensitive information.

8 Disclosure of information by email:

8.1 Personal or sensitive information is at risk if sent outside of the Council's network.

8.2 If an e-mail is sent to an address that is not a Council domain address the email will be delivered through the public network and the message may be left at several locations on its journey and could be deliberately intercepted.

8.3 Email should not be used for sending personal or sensitive information unless technical measures are in place to keep the message secure.

8.5 The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent and alternative methods should be used.

8.6 No identifiable personal information should be included when sending on emails.

8.7 The recipient of Gamlingay Parish Council emails are prohibited from being forwarded, copied or blind copied to any third party within or outside of the Council.

8.8 Any Councillor email contact with a member of the public shall be directed to the Councils Office for the attention of Gamlingay Parish

9 Sharing of Personal Information

9.1 Information relating to individuals shall not be shared with other authorities without the agreement of the Data Control Officer.

9.2 Staff should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.

Appendix I - The Caldicott principles

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary
Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for individuals to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis.
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities.
Action should be taken to ensure that all those handling personal confidential data are made fully aware of their responsibilities and obligations to respect an individual's privacy.

6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.