Framlingham Town Council

Information Protection Policy

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 Framlingham Town 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 Framlingham Town 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

2.3 For the purpose of this document, “Personal Information” means any information from which the identity of a private individual can be inferred directly or indirectly. Such information must be processed only subject to the terms of the GDPR, and only subject to “Consent” as defined in GDPR, except where there is alternative lawful basis for processing. For example, Town Councillors including the Chair are deemed to have given Consent for matters concerning the Town Council.

3 Information Storage

3.1 All electronic information will be stored in a manner consistent with §3.7, and regular backups will be made. There will be at least two backups used alternately, or a similar scheme employed that protects against a double failure.

3.2 Information will not be held that breaches the Data Protection Act (1998) or formal notification and guidance issued by Framlingham Town 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 Framlingham Town Council as a potential security risk should not be stored on a network, except for networks that have been assessed as meeting the security requirements of this Policy. To facilitate this Framlingham Town 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 that may contain personal or sensitive information from premises without the express consent of the information owner. Consent will only be given in exceptional circumstances. A booking out/in system shall be considered.

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 Framlingham Town Councils disposal policy.

4.5 Distribution of material that may contain personal or sensitive information should be via the most secure method available.

5 Telephone calls that may relate to personal or sensitive information:

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

5.2 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).

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

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

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

6 Fax transmissions that may relate to personal or sensitive information:

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

7 Email communication that may relate to personal or sensitive information:

7.1 Personal or sensitive information is at risk if sent outside of the Council's network. If it is necessary to send such information outside the Council's network then secure email should be used whenever possible.

7.2 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.

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

7.4 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.

7.5 No identifiable personal information should be included when forwarding emails unless the forwarded email also complies with the clauses in this section.

7.6 Any Councillor email contact with a member of the public shall be directed to the Councils Office for the attention of the Town Clerk

8 Sharing of Personal Information

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

8.2 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.