FRAMLINGHAM TOWN COUNCIL

INFORMATION SECURITY, PROTECTION, AND REMOVABLE INFORMATION STORAGE POLICY

1. Overview

Framlingham Town Council processes a large amount of data and this policy defines how it needs to be protected.

2. Information Security.

All information is at risk from being lost damaged or misplaced. In addition, the Town Council's IT systems are at risk from attacks or unauthorised use.

2.1 Information going to the wrong person or place

The most common mistake is to send an email to the wrong person or cc-ing someone who should not have been copied in. The golden rule is to act quickly and escalate the knowledge of the mistake upwards within The Council. A rapid full and honest apology from the person making the mistake is required and if this is not accepted, then the Council will have to decide what to do. Ultimately the issue could form part of an investigation leading to prosecution under the GDPR Act.

2.2 Loss of information

Files can be accidentally deleted. For this reason, all The Council laptops should be backed up to an external hard drive on a weekly basis. This will not recover very recent information but minimises the risk. The back up media must always be kept locked away.

2.3 Information or systems being attacked by external third parties.

The Town Council supplies a virus protection and firewall software for all laptops. E-mails with attachments from unknown people should not be opened without being scanned by the anti-virus programme. Passwords to IT systems should never be given to any third party, and all computers must be password protected. All information that contains sensitive or personal information must also be encrypted with the Vera Crypt software.

Any suspected attack on the Town Council IT system should be **immediately** reported to the Data Protection Manager – The Town Clerk

3. Removable Media

Removable media is classified as Memory Sticks and CDs. Removable media is a high-risk system for sensitive data. Removable media must be kept locked up when not in use. Best practise is to password protect documents and if passing information within the Town Council to verbally tell the person who is being given the media the password.

4. Personal use of Town Council IT systems by staff and Councillors.

In most cases this is not permitted during working hours, except by express permission of the Town Clerk in an emergency.