

# Lowestoft Town Council

## Policy for the Secure Use of USB Memory Sticks

### 1.0 Introduction

- 1.1 The policy provides guidance to staff on the secure use of USB memory sticks for carrying confidential, sensitive and Person Identifiable Data (PID) including data on service users, councillors & staff.
- 1.2 USB memory sticks have become increasingly popular because of their small physical size and large storage capacity. This has made them very convenient devices for carrying files from one place to another. However, these very features have introduced new information security risks:
- Loss of information – a memory stick, like a computer, is susceptible to data loss or failure.
  - Potential breach of confidentiality – if the memory stick is lost or stolen.
  - Physical loss – being so physically small the memory stick can be easily lost.
  - Corruption of data - if the memory stick is not removed from a computer properly.
  - Virus transmission – memory sticks can introduce viruses onto a computer network.

### 2.0 Reducing the Risk of Losing Information

2.1 There are two main ways of preventing the loss of information:

- Avoid physically carrying such information

And

- Encrypting confidential, sensitive & Person Identifiable Data

#### Avoidance

2.2 Confidential, Sensitive and Person Identifiable Data must not be stored or carried on non-encrypted memory sticks. Staff should use other secure methods for carrying such information.

#### Encryption

2.3 An encrypted memory stick allows information to be stored but renders the information undecipherable unless the correct password is entered. Encrypted memory sticks will be issued to specifically named members of staff for their professional use. They must not share the device with other persons. They must not share or disclose the password to other persons.

#### **NB**

***Confidential, sensitive or PID carried on encrypted memory sticks must not, under any circumstances, be placed on non-Lowestoft Town Council issued computers. Such information must always remain on the encrypted device and be immediately transferred to the L Drive or users' personal drive and deleted from the encrypted memory stick once no longer required to be on the device.***

### 3.0 Asset Register

3.1 An asset register will be maintained of all encrypted memory sticks issued. All issued encrypted memory sticks remain the property of Lowestoft Town Council and must be returned when staff leave employment with Lowestoft Town Council or no longer need to use such a device.

### 4.0 Responsibility

4.1 All staff have a duty of care to ensure all confidential, sensitive and PID is held securely at all times. The loss of confidential, sensitive and PID information is extremely serious and if a member of staff is found to be using a non-encrypted memory stick for carrying confidential, sensitive and PID information they may be subject to disciplinary procedures. All losses of confidential, sensitive and PID must be reported to the Town Clerk.