NORTH WALSHAM TOWN COUNCIL

Mobile Device Policy

Adopted by the Council at its meeting held on 25.2.20

1 Introduction

1.1 Council purchased and leased mobile devices are Council property and are only issued for use for Council purposes.

2 Security, Loss and Theft

2.1 All mobile devices must be signed for by a user before removal from Town Council premises and countersigned by the Town Clerk who will also record the return of the device.

2.2 Mobile devices must be kept securely at all times.

2.3 If a Council owned mobile device is lost, this should be reported to the Town Clerk as soon as possible.

2.4 If a Council owned mobile device has been stolen, then it is the user's responsibility to report the theft to the Police as a matter of urgency. The Police will provide a Crime Reference Number which needs to be submitted to the Town Clerk.

2.5 Should evidence exist to suggest that an employee's negligence has led to the loss of the mobile device, or if they fail to follow the correct procedures for reporting the loss, action may be taken under the Council's Disciplinary Procedure.

3 Information security when using mobile devices

3.1 No personal, sensitive or business critical information may be stored on Council issued tablets, smartphones or mobile phones.

3.2 Mobile devices must not be used for permanent storage of large amounts of information. All information saved to a mobile device must be transferred to the Council network and be removed from the mobile device as soon as practicable in order to minimise the amount of corporate information held outside of the corporate network.

3.3 Care must be taken when using mobile devices in public places, meeting rooms and other unprotected areas outside of the Council's premises. When viewing information on a mobile device in public places ensure that care is taken to avoid the risk of information disclosure by being overlooked by unauthorised persons.

3.4 Tablets and smartphones will be issued with a screen lock PIN code and password. The PIN protected screen timeout will be set to 5 minutes or less of inactivity. Devices must be locked or switched off when not in use.

4 Physical Security of Mobile Devices

4.1 All mobile devices must be maintained in an environment with an appropriate level of security to prevent unauthorised access to information stored on the device, or theft of the device itself.

4.2 When not in use all mobile devices must be retained in a secure environment. This may include a lockable store cupboard with controlled access, or lockable metal cabinets in larger alarmed offices, with controlled access.

4.3 Users must ensure that they take adequate precautions to protect mobile devices against theft or accidental damage at all times.

4.4 A mobile device must not be left unattended while it is connected to a computer.

4.5 A mobile device must not be left unattended in public.

4.6 Mobile devices must not be left in an unattended vehicle at any time.