MACCLESFIELD TOWN COUNCIL

Bring Your Own Device (BYOD) POLICY

DOCUMENT VERSION CONTROL

Document Title: BYOD Policy

Version No.	Date Change Made	New Version No.	Changes Made By (initial)	Comment
00.01	May 2018		HW	New policy for GDPR

Table of Contents

Introduction

Macclesfield Town Council grants Councillors and Officers the use smartphones and tablets of their choosing for council business.

This policy is intended to protect the security and integrity of personal data controlled and processed by Macclesfield Town Council.

Macclesfield Town Council reserves the right to revoke this privilege if Councillors and Officers do not abide by the policies and procedures outlined below.

Macclesfield Town Council Councillors and Officers must agree to the terms and conditions set forth in this Bring Your Own Device (BYOD) policy in order to be able to connect their devices to the company network.

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed
- Tablets including iPad and Android are allowed
- Laptops are allowed
- Connectivity issues may be supported by ICT services but this will be on a case by case basis. In the first instance the connectivity issue should be reported to the Clerk.
- The device manufacturer or their carrier should be contacted for operating system or hardware-related issues.

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- Passwords must be at least six characters and a combination of upper- and lower-case letters with a number and a symbol.
- Passwords must be kept confidential and must not be shared with family members or third parties.

- Passwords must be changed if it is disclosed to another person or discovered.
- Devices must be encrypted
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Home Wi-Fi networks must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.
- Public data backup and transfer services (Dropbox, Google Drive, must not be used
- Data must only be stored on internal memory, never on a removable memory cards
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- All data relating to Macclesfield Town Council will be erased at the end of a Councillor's term or in the case of an Officer at the end of his or her employment.
- All data relating to Macclesfield Town Council will be erased if there is a personal data breach
- All data relating to Macclesfield Town Council will be erased if there is a virus or similar threat to the security of data.
- Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using Wi-Fi facilities in public places (e.g. coffee shops or airports), or otherwise. Some apps for smartphones and tablets may be capable of accessing sensitive information.

Risks/Liabilities/Disclaimers

- Lost or stolen devices must be reported to Macclesfield Town Council within 24 hours. Councillors and officers are responsible for notifying their mobile carrier immediately upon loss of a device.
- Councillors and officers to adhere to the Macclesfield Town Council's BYOD policy as outlined above.
- Councillors and officers are personally liable for all costs associated with his or her device.
- Macclesfield Town Council reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.