Filey Town Council
Council Offices, 52A Queen Street,
Filey, North Yorkshire, YO14 9HE
Telephone: 01723 514498
Email: mail@fileytowncouncil.co.uk
Website: www.fileytowncouncil.co.uk

Bring Your Own Device Policy

Document History

Adopted by Council on 23 May 2018
Reviewed 9 May 2019, May 2020 & May 2021
To be reviewed – May 2022

David Liddle
Town Clerk & Responsible Financial Officer

1. INTRODUCTION

1.1 The use of personal mobile devices, such as smartphones, laptops and tablets in connection with Town Council's business is a privilege granted to specific employees through approval of their management.

1.2 The Council reserves the right to revoke these privileges if Users do not abide by the policies and procedures set out in its 'Bring Your Own Device Policy' (BYOD) Policy.

1.3 These policies are in place to protect the integrity and effective operation of the Council's data, information and communications systems to ensure they remain safe, secure and available for carrying out the Council's business, including:

- To protect devices and systems from downtime, caused by malware and viruses.
- To protect systems and information that is necessary to business processes, which would present risk to the operational requirements of the business.
- To protect information where access must be restricted to certain groups or individuals.
- To protect the value of the information to the company e.g. intellectual property, commercially sensitive information.
- To protect confidential information because of legal obligations, such as personal data under the Data Protection Act or payment card PCI-DSS regulations.
- To protect information included in regulatory requirements, such as financial data.
- To protect information that is externally owned or provided, such as those defined in contracts.
- To protect information that is important to health and safety.

1.4 This policy document covers the many areas, in a simple and concise format, which are necessary to manage and secure our BYOD environment while enabling you to be more productive.

2. USER ELIGIBILITY

2.1 The Council's BYOD policy applies to all employees that use personal devices and to consultants and other temporary workers, who require access to specific systems to carry out their duties.

2.2 The Council may limit what data or systems that can be accessed by personal owned devices.

2.3 Users with personally owned devices can access the following list of applications according to their role within the company, and the type of personal device: **Office 365**.

2.4 The User must understand the consequences of installing personal applications on personal devices used to access the Council's networks, information and communications systems. These can introduce malware into systems, or result in exposing confidential data held, to theft or loss.

2.5 Best practise includes:
- Use only well-known and well-respected application vendors.
- Use any Council App repositories intended for personal devices. From time to time the Council may sign up to popular Mobile apps used by employees.
- Maintain up-to-date security software on personal device(s).
- Automatically run/accept regular updates of the application software Privacy the Council is committed to protecting the privacy of Users enrolled in its BYOD programme.

2.6 The Council will permanently delete all its records of an inadvertent contact with a User's personal data and inform the User as soon as discovered and practical.

2.7 The Council will never search a User's device data without the prior consent of the User.

2.8 If the User device has been contaminated with malware, which presents a risk to the Council's data and its systems, then it has the right to wipe the whole device, which may result in the loss of personal and business data. the Council will make every effort to communicate with the User BEFORE these actions are taken.

2.9 The Council disclaims any liability for loss of personal applications or data, whether directly or indirectly resulting from the usage of company information and communications systems, and/or the wiping of company apps or data, or the removal of malware or the wiping of the whole device.

2.10 The Council does not accept any financial responsibility for mobile phone, mobile data and public WIFI services incurred by the User.

2.11 The User is responsible for reporting lost or stolen devices or breaches of security on personal owned devices to the IT Service Desk in the first instance.

2.12 Upon leaving employment the **User MUST** remove all Council information, applications, passwords, data and APPs from personally owned devices upon separation from the Council or at the Council's request.

2.13 The Council may/will require checking and/or wiping of any company data held on personal devices.

2.14 Any Council owned, licensed and installed software on personally owned devices is required to be reconciled. Depending on the type of license:
- The Council may request the User to reimburse the Council for the software, or
- The Council may request the User destroy the software, or
- The Council may decide to allow the User to keep software with no further value.

2.15 The IT Service desk will only support company applications, network and User access/login to the Council's systems, and company software/configuration installed on personal devices.

2.16 The Council will not support any mobile applications for personal use and consumption.

2.17 The Council will not provide support for broken personal devices.

2.18 The Council reserves the right to revoke the privileges to use personal devices if Users do not abide by the Council's policies and procedures

2.19 If the User circumvents configurations, security, access and practices then the User will be in violation of the Council's BYOD Policy.

2.20 Personal device will/may be wiped of Council data if a policy breach is detected

2.21 Policy violations will/may be subject to warnings or disciplinary action as per the Council's Terms and Conditions of Employment.

3. DEVCIE REGISTRATION AND COMPLIANCE

3.1 The User must ensure that personal owned devices are registered and have received consent to connect to the Council's network, information and communications systems. This will ensure that devices are set up correctly and that the User and their device(s) comply with the Council's BYOD Policy.

4. USER AGREEMENT AND RESPONSIBILITIES

4.1 **The User MUST** comply with the Council's BYOD policy terms and conditions.

4.2 **The User MUST** contribute to the protection of the Council's data, applications, information and communications systems by exercising caution, being aware of the risks, complying with the Council's security requirements and security best practices.

4.3 The Council retains ownership of all the business data, documents and files, intellectual property and secure-access information and has the right and obligation to govern this data.

4.4 The User agrees that the Council may require them to implement specific device configurations or software before the User is allowed access to Council data, applications, networks, information and communications systems. If the User disagrees with any of these requirements, they will not be allowed access from their own device(s), or may only gain access to certain systems, or may only be given guest access to the Internet.

4.5 The Council and the User must comply with all regulations and laws. These laws and regulations might require the Council to access its data on your personal device(s), or you may be compelled to provide or remove any such data from your personal device(s).

5. ACCEPTABLE USE

5.1 **The User MUST** follow all administrative and acceptable use policies when a personal owned device is connected to the Council's networks,

information and communications systems or where social media and/or collaboration solutions are applied for business purposes.

5.2 **The User MUST** ensure that when they use their personal device for personal reasons, that they are not using the Council's intellectual property rights, any business confidential data, or any data that may be regulated or protected under European or UK legislation.

5.3 The Council retains the right to perform operations on a personally owned device, such as scanning for malware, or checking security configurations. The User will be made aware of how and when these operations will be carried out.

5.4 Users who do not wish to have the required operations undertaken on their device, will not be allowed to access the Council's networks, information systems, applications and data.

5.5 **The User MUST** consider the sensitivity of the Council's data held on the personal owned device, when sharing the device with family and friends.

5.6 **The User MUST** report **IMMEDIATELY** any data breaches, disclosures or malware infections on personally owned devices to the Council immediately they become aware.

5.7 As a condition of access to company data and ICT resources, the User is required to install security software and activate the devices firewall or install the Council's chosen security software.

5.8 The User MUST regularly update and/or accept updates to OS software directly provided by the devices manufacturer or service provider.

5.9 If the User device has been contaminated with malware, which presents a risk to the Council's data and its systems, then it has the right to wipe the whole device, which may result in the loss of personal and business data. The Council will make every effort to communicate with the User **BEFORE** these actions are taken.

5.10 Jailbreaking, rooting and modifications to the personal device OS are **PROHIBITED**.

5.11 **The User MUST** back-up or synchronise any company data/information held on their personal device with company systems.

5.12 **The User MUST** ensure that any device that is to be replaced or thrown away must have the permanent memory wiped.

6. LOGINS, PASSWORDS, PINS AND AUTHENTICATION

6.1 The Council will issue Logins and Passwords for access to its network, applications, information and communications systems - as it does with company-owned devices. This information MUST never be passed on to third parties or communicated on personal social networks.

6.2 The User **MUST** ensure there is a PIN or Login to operate any personal owned devices before access to the Council's networks, information systems, applications and data can be granted.

6.3 The Council may require device PINs and passwords to be changed regularly, to comply with its security policies, regulatory or legal requirements.

6.4 The Council may enforce the use of passwords for personal owned devices to comply with its policy or any data governance.

6.5 The Council may block access for devices with out-of-date passwords, or passwords with a low strength.

6.6 Where the Council uses additional security techniques to secure its data and systems, such as two-factor authentication, the User **MUST** use such systems with their personal device where directed.

6.7 The User has a responsibility towards the safeguarding of company and confidential data in their possession. It is best practice to encrypt confidential data on mobile devices in case of loss or theft.

6.8 Where the Council must comply with industry regulations and legislation, the User MUST encrypt all confidential data held on mobile personal device(s). In these circumstances the company has the right to monitor, check and prevent access for any devices without encryption.

6.9 The Council may manage and monitor personal devices of a User enrolled in the Council's BYOD programme, to support its data security policies and compliance requirements.

6.10 The User should allow any the Council's appointed 3rd party organisation access to the personal device for audit and checking purposes.

6.11 The Council may deploy software on personal devices of an enrolled User so that they adhere to the Council's platform and operating system (OS) version policy or security policies.

6.12 The Council will inform the User about any device management and policy enforcement processes that it does/will apply.

6.13 If a User does not want their personal device to be managed or have policies enforced, then they may/will not be allowed access to the Council's network, information and communications systems, or the User may be given limited access to company systems.