**Democratic Services**
**White Cliffs Business Park**
**Dover**
**Kent CT16 3PJ**

**Telephone:** **(01304) 821199**
**Fax:** **(01304) 872452**
**DX:** **6312**
**Minicom:** **(01304) 820115**
**Website:** **www.dover.gov.uk**
**e-mail:** **democraticservices@dover.gov.uk**

4 May 2022

Dear Councillor

I am now able to enclose, for consideration at the meeting of the **CABINET** on Monday 9 May 2022 at 11.00 am, the following reports that were unavailable when the agenda was printed.

5 **BRING YOUR OWN DEVICE POLICY** (Pages 2-10)

To consider the report of the Head of Community and Digital Services.

Responsibility: Portfolio Holder for Finance, Governance, Digital and Climate Change

10 **RESTORATION OF MAISON DIEU, DOVER** (Pages 11-50)

To consider the report of the Strategic Director (Operations and Commercial).

Responsibility: Portfolio Holder for Community and Corporate Property

Yours sincerely

Chief Executive

| | |
|---|---|
| **Subject:** | **BRING YOUR OWN DEVICE (BYOD) POLICY** |
| **Meeting and Date:** | **Cabinet – 9 May 2022** |
| **Report of:** | **Brinley Hill, Head of Community and Digital Services** |
| **Portfolio Holder:** | **Councillor Chris Vinson, Portfolio Holder for Finance, Governance, Digital and Climate Change** |
| **Decision Type:** | **Executive Non-Key Decision** |
| **Classification:** | **Unrestricted** |
| **Purpose of the report:** | To allow DDC staff to use personal smart devices to access DDC Microsoft 365 applications and data. |
| **Recommendation:** | To approve a new project and policy implementing processes and security enabling staff the flexibility of using personal smart devices for work. |

## 1. Summary

1.1 This project will allow DDC staff to utilise personal mobile phones/tablets (smart devices) for work purposes, giving greater flexibility of working and potentially saving DDC money in handset replacements. Phase 1 of the project will be DDC employees initially, we will then look to extend the project to include rolling out Bring Your Own Device (BYOD) scheme to Members. The Portfolio Holder for Finance, Governance, Digital and Climate Change is currently on the BYOD pilot scheme.

## 2. Introduction and Background

2.1 DDC currently has over 300 mobile phone contracts for staff. The contracts purchased are SIM only and DDC purchases handsets (i.e. mobile phones) separately. Giving better flexibility of contracts.

2.2 Approximately every 5 years these handsets must be replaced due to handset models only being supported by the manufacturers for this time. After this period, security updates and applications used by DDC are no longer supported. The cost of replacing this number of handsets is £96,000.

2.3 Utilising a range of security options included in DDC's Microsoft 365 subscription, staff are able to securely access work applications such as Microsoft Teams, Outlook, Word and Excel on their personal phones/tablets.

2.4 The SIM-only contracts o2 provide to DDC can also be added to their personal phones using eSIMs (a virtual SIM card). These are added as a second number onto their phones and can be turned on/off separately to their personal number, allowing them to effectively turn off their work number out of hours.

2.5 A Bring Your Own Device (BYOD) policy (see Appendix 1) has been created for approval to allow staff to make use of the functionality o2 and Microsoft provides.

3. **Identification of Options**

3.1 Stay as is – Do not adopt BYOD policy.

3.2 Approve BYOD policy to enable staff the option of using personal devices for work.

4. **Evaluation of Options**

4.1 The option to continue not allowing BYOD has been considered. Continuing without BYOD will cost DDC more money in mobile handset replacements and mean they have to carry around multiple mobile phones.

4.2 As well as enabling staff to work more flexibly using their own mobile devices. This policy will save DDC some of the cost of replacing mobile handsets and will create less waste. The recommendation is to approve the BYOD policy.

5. **Resource Implications**

5.1 The security functionality required to enable BYOD in a secure way is already included in DDC's Microsoft 365 subscription, there will be no cost in implementing this.

5.2 Using forms and automation in 365, the process in enabling staff to request the ability to use their own device and enable it will not require a lot of staff time. This can be enabled by Digital Services.

6. **Climate Change and Environmental Implications**

6.1 The Climate Change Officer has been consulted in preparation of this report and has highlighted that Bring Your Own Device will have the advantage of reducing waste.

7. **Corporate Implications**

7.1 Comment from the Section 151 Officer (linked to the MTFP): Accountancy has been consulted on the report and have no further comments to add. (LS)

7.2 Comment from the Solicitor to the Council: The Solicitor to the Council has been consulted in the preparation of this report and has no further comments to make.

7.3 Comment from the Equalities Officer: This report does not specifically highlight any equality implications, however in discharging their duties members are required to comply with the public sector equality duty as set out in Section 149 of the Equality Act 2010 http://www.legislation.gov.uk/ukpga/2010/15/section/149

8. **Appendices**

Appendix 1 - BYOD Policy

9. **Background Papers**

None.

Contact Officer: Abi Robinson, Digital Services Manager

**Bring Your Own Device Policy for Dover District Council**

**You must complete the form at the link below if you agree to adhere to this policy, and your manager has given approval.**

**https://forms.office.com/r/JjPV36D1ET**

## Introduction

The Council's move to Microsoft 365 productivity platform will enable the opportunity to allow staff to use their own personal mobile devices for work purposes. This Bring Your Own Devices (BYOD) approach is being used more frequently within the public sector and has been commonplace within the private sector for some time.

This Policy sets out the conditions for the use of BYOD, and the restrictions and risks users must be aware of when deciding whether to use their own device for work purposes.

The Policy is intended to protect the security and integrity of the Council's data and technology infrastructure, whilst enabling staff to work in the most productive and effective ways possible. Devices that are shared – such as with other family members – cannot be used as a BYOD as there is an increased risk of information accidently being accessed by unauthorised users.

While using your own device you must follow the Council's key policies, including the Internet Use Policy and the Email Use Policy.

This Policy covers the following smart devices only:

- Mobile Phones
- Tablets
- Ancillary Mobile Devices, e.g. Smart Watches

Personal computers **cannot** be used to access your Microsoft 365 account, please continue to take your work device with you to work remotely.

## Constraints and Risks

The Council, regardless of devices used for work purposes, has a duty to protect information. Failure to protect and manage personal data can lead to significant fines for the Council and exposure to claims for damages. Therefore, this policy operates within the scope of the wider data protection policies the Council has adopted.

**Applications in Scope**

Only apps in the following list are permitted to access corporate data from personal devices. These apps can be downloaded from either Apple's App Store or Google's Play Store. Direct access to your account via web browser is not permitted as it allows you to bypass security built into the App. Other work-based applications that are required to deliver a specific role or functions will only be available on Council owned and managed devices.

Information held within the 365 applications is held securely within a Cloud environment. Any data cached on the device's storage is automatically stored in a separate encrypted container on the device. This container can be remotely wiped from the device by DDC (without affecting your personal information on the device).

| App Name | OS |
|---|---|
| Microsoft Edge | iOS/Android |
| Microsoft Excel | iOS/Android |
| Microsoft Lists | iOS/Android |
| Microsoft Office | iOS/Android |
| Microsoft OneDrive | iOS/Android |
| Microsoft OneNote | iOS/Android |
| Microsoft Outlook | iOS/Android |
| Microsoft Planner | iOS/Android |
| Microsoft Power Apps | iOS/Android |
| Microsoft Power BI | iOS/Android |
| Microsoft Power Automate | iOS/Android |
| Microsoft PowerPoint | iOS/Android |
| Microsoft SharePoint | iOS/Android |
| Microsoft StaffHub | iOS/Android |
| Microsoft Stream | iOS/Android |
| Microsoft Teams | iOS/Android |
| Microsoft To-Do | iOS/Android |
| Microsoft Visio Viewer | iOS/Android |
| Microsoft Whiteboard | iOS/Android |
| Microsoft Word | iOS/Android |
| Yammer | iOS/Android |

**Accessing Public Sector Network (PSN) data**

Staff that access data sourced from the Public Sector Network (PSN) should be aware that BYOD is not always an appropriate option for accessing that data.

If you regularly send or receive emails containing sensitive information sourced from PSN Connected Services (e.g. Whitehall departments, Police, NHS and Public Health England) you should consider whether any agreements you have with those organisations permit you to use BYOD and not a 'fully managed' device provided by the Council.

**Personal Data**

Periodically users of work accounts on BYOD will be forced to sign back into their account using their work credentials. This additional layer of security ensures your Council data is not being accessed by unauthorised users.

While your personal data should be unaffected by enrolling your device in BYOD, it is your responsibility to back up your personal data and information to prevent data loss.

**Please note: The Council's Corporate Information Governance Policies apply to Bring Your Own Device (BYOD) Please refer to these policies when processing Council information and personal data.**

**Exclusions and Restrictions**

For the purposes of this policy, Bring Your Own Devices includes the following categories of personal device:

- Mobile Phones
- WiFi and Data Tablets
- Ancillary Mobile Devices e.g. Smart Watches

**Devices that are shared – such as with other family members – cannot be used as a BYOD and will not be approved, as there is an increased risk of information accidently being accessed by unauthorised users.**

**Once enabled as a BYOD device you must not permit use of your device by others even though you would not normally regard it as a shared device.**

Devices specifically excluded from this Policy include, but are not limited to:

- Personal Computers (PCs)
- Laptops/MacBooks
- Chromebooks
- Smart Home Devices e.g. Internet enabled TVs, Smart boxes/devices
- Gaming devices and voice controlled smart devices
- External storage devices, e.g. USB flash drives, hard drives and memory cards

All devices are subject to review and amendment at any time, and employees should ensure that when they change a personal device for BYOD purposes, they review the Policy for changes and amendments.

Input devices (such as keyboard and mouse) and monitors are not included in the BYOD policy.

**Management of Bring Your Own Smart Device**

In order to manage data and access to information through the use of BYOD, all apps in the permitted list above which are logged into with a DDC MS365 account will be subject to the Mobile App Management (MAM) protection policies deployed via Microsoft Intune. This system gives the Council the ability to apply restrictions on the app, for example, blocking copying and pasting from a work app to a personal app. Details of applied restrictions can be found later in this policy. DDC reserve the right to remove DDC apps and data related to a staff member's work account. If a device is lost or stolen, the Council will be able to remotely remove, delete and/or block access to the apps related to the work account.

**Terms of use**

Microsoft Intune MAM (Mobile App Management) is used to secure corporate apps/data on your device. By installing permitted apps on your device and signing in with your DDC account, you accept that the Council has the access and ability to remotely delete corporate apps and work-related information, data and accounts. DDC retains control over any Corporate apps/data but has no visibility/control of other apps/data stored on the device, Intune creates an encrypted area on your device to keep corporate and personal data separate. DDC will not have access to the location of your device, if the device is lost, you can still use your IOS/Android "Find My Device" feature.

The Council accepts no liability for costs associated with the operation and servicing of the device.

The Council does not and will not monitor personal usage of your smart device, but can monitor the usage of the corporate apps/data on the smart device. This information will also detail the make of the device, operating system in use, and last log in to the corporate account, it will also require a PIN to be set if one is not already enabled. No further information is held or can be accessed by any individual working for either the Council or EKServices.

**Lost or stolen devices**

Lost or stolen devices must be reported to ICT within one working day, if you are out of the country please report this as soon as possible and make your manager aware. If your device is stolen please report this to the police to obtain a crime reference number.

This will be classified as a Personal Data Breach under GDPR and will require you to report it internally at ICT Portal - Report a Data or Cyber Security Breach (topdesk.net).

Staff are responsible for notifying their own insurers and contract suppliers in the event of their device being lost or stolen.

**Security of BYOD**

In order to prevent unauthorised access to corporate accounts and information, you will be prompted for a 6 digit PIN to be set for access to protected apps. You will not be able to access your work accounts and information in protected apps without PIN enabled. Failure to protect your apps on the device and the information held on it, or accessed by it, will result in the corporate accounts being removed from the mobile device. Once set, 5 incorrect app PIN attempts will wipe all corporate data from the device.

Your pin must not be as simple as 111111 or 123456. You must have a strong and complex passcode.

For you to use your personal device it must be password protected. If your device has no password set, you will not be authorised to use it to access Council data.

**Manufacturer support and updates**

Devices must be running an Operating System supported by the manufacturer, if running an unsupported version your device cannot be used for BYOD.

Users must ensure their device is able to be updated regularly with operating system updates and security patches. Devices that are not running up to date operating systems may be blocked from accessing Council work accounts and information without any advance notice.

Jailbreaking, rooting and modifications to the device are prohibited.

**Device Support**

Dover District Council will not provide support for devices should they fail; staff are encouraged to ensure they have sufficient insurance to protect against theft, loss or damage.

Information from Council accounts, apps and communications must not be downloaded onto a mobile device's internal memory or personal backup service, as this poses a security risk to the Council as well as Data Protection risks.

**Network Access**

BYOD can be used to access the Council's secure WiFi , which will only give internet access and not access to on premise infrastructure.

If you are aware of, or are concerned about, a potential security breach to your personal device – such as from a phishing email or virus attack – you should contact EKS ICT helpdesk as soon as possible, and not access your work account until EKS ICT have advised of any risks, breaches or fixes.

**Ancillary devices**

BYOD must not be charged by plugging into a Council laptop, PC or docking station. Only tested and authorised USB plug adapters are to be used to plug into the Council's power supply.

There are a growing number of smart devices that can be linked/paired with tablets and mobile phones to pass information, such as emails and meeting alerts, to the connected device via WiFi or bluetooth. These include devices such as Apple Watch (for iOS) and smart watches (e.g. a Fitbit)), use of these devices is acceptable but will be managed under the same policy, guidance and restrictions for use as other acceptable devices.

**Liabilities**

The Council accepts no liability for any damage or costs incurred or associated with the operation, maintenance and servicing of a personal device under this policy.

While the Council and EKS will take every precaution to prevent personal data from being lost in the event a work account is removed from a personal BYOD, it is the employee's responsibility to ensure precautions and measures are in place to backup and recover personal information and any installed personal apps.

The Council reserves the right to take appropriate disciplinary action in line with the Council's existing policies and guidance for non-compliance with this policy.

**Equalities & Diversity**

The Council will take reasonable steps to ensure the BYOD policy is accessible to all of its staff. This may include changing the way some aspects are delivered to staff with disabilities for example. Should a member of staff have particular needs in respect of any of the 'Protected Characteristics' defined within the Equality Act 2010, they are encouraged to discuss these with their Line Manager.

**Restrictions applied to the apps**

The following app protection policy restrictions will be applied automatically to the apps when you log in to them using your DDC MS365 account.

- Backups of corporate data to iCloud / Google accounts will be blocked.
- Corporate data can only be sent between protected apps.
- Saving of files restricted to only OneDrive/SharePoint.
- Opening of files restricted to OneDrive/SharePoint and camera.
- Cut/copy and paste out to other protected apps only.
- Do not display corporate data in notifications. If not supported by the application, notifications are blocked.
- Web links from corporate apps can only be opened in Microsoft Edge browser app.
- Screen capture of protected apps will be blocked (Android only).
- Jailbreaking the device will cause the device to wipe corporate data.

**Only Android or Apple devices are supported for BYOD.**

**Policy Review**

This policy will be reviewed every year, or earlier at the request of either staff or management, or in light of any changes to legislation or national guidance.

Please contact the digital or data protection team for any advice or guidance.

April 2022

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

Document is Restricted

Document is Restricted