Information Security Document

Mobile Working Procedures

Version 10.0

Version	Date	Detail	Author
1.0	02/03/2011	Completed for distribution	Jo White
1.0	26/05/2011	Approved by Information Governance Group	Jo White
2.0	22/06/2012	Reviewed by Information Governance Group. Approved by email due to meeting being cancelled.	Jo White
3.0	31/07/2013	Reviewed by Information Governance Group. Links corrected. Point 32 added.	Jo White
4.0	11/08/2014	Reviewed by Information Governance Group.	Jo White
5.0	12/10/2015	Reviewed by Information Governance Group	Jo White
6.0	09/01/2017	Reviewed by Information Governance Group	Jo White
7.0	05/03/2018	Reviewed by Information Governance Group. Name changed to remove Teleworking.	Jo White
8.0	08/04/2019	Reviewed by Information Governance Group. Direct Access and Microsoft Outlook app added.	Jo White
9.0	12/05/2020	Reviewed by Information Governance Group. Volunteers added.	Jo White
10.0	08/06/2021	Reviewed by Information Governance Group.	Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
A.6.2.1 > 2	Mobile computing and Teleworking
A.8.3.2	Disposal of media
A.8.2.3	Handling of assets
A.9.3.1	Use of secret authentication information
A.11.1.5	Working in secure areas
A.11.2.1	Equipment siting and protection
A.11.2.6	Security of equipment and assets off-premises
A.11.2.8	Unattended user equipment
A.13.2.1	Information transfer policies and procedures

1. Introduction

The Council's use of Information Communications Technology enables its workforce to access its ICT systems, services, information and data while away from normal working environments and in remote locations.

Mobile (remote) working is defined as working in a place that is not an individual's normal work base, which could be at home, a touchdown centre, Council provided guest Wi-Fi hotspots, hotels, airports, conferences – anywhere a connection to a public communications network makes access via secure portals to Council resources possible.

Webmail is a method of accessing Council email from a PC or mobile device which has access to the internet via a secure, encrypted web browser session.

Working from home, whilst travelling, at a client's site or at any other location away from the established (physical) office may be attractive and offer benefits. However, opening up the Council's information and systems whilst mobile working also presents security risks. Intruders (hackers, electronic eavesdroppers, shoulder surfers etc) may be able to access, read and potentially modify Council information and systems without having to be on site.

2. Purpose

The purpose of these procedures is to ensure that the security of information and systems, accessed through mobile working, is given due importance. It is essential that staff have knowledge of the Council's security procedures and policies and they are accepted, understood and adhered to.

These procedures have been produced to ensure that the protection of personal and sensitive data is maintained in accordance with the Data Protection Act 2018 and the Council's information security policies and procedures whilst Council staff are undertaking remote working in its many forms.

3. Scope

The scope of these procedures includes all persons/parties who have access to Council information and ICT systems belonging to or under the control of Derbyshire County Council including:

- Council employees
- Elected Members
- Third Parties
- Temporary staff
- Partner organisations
- Members of the public
- Volunteers
- Any other party utilising Council ICT resources

Under the property rationalisation programme the following three types of flexible worker profiles are included within the scope: flexible worker, mobile worker and field worker.

Processing devices that can be used as part of mobile working include:- PCs (touchdown centres etc), laptops and notebooks, tablet PCs, smart phones, digital

cameras, mobile phones and any other mobile device that record and/or process information.

Removable media (e.g. CDs, DVDs, SD cards, flash drives/USB data sticks, portable hard drives etc.), is anything on which information and data can be copied, stored, accessed and/or shared on other computing devices.

4 . Responsibilities.

Directors are responsible for ensuring that all staff and managers are aware of security policies and that they are observed. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems. Designated owners of systems, who have responsibility for the management of ICT systems and information, need to ensure that staff are aware of their responsibilities towards security. Designated owners of systems and information need to ensure they uphold the security policies and procedures.

Users must have read the guidelines which advise the correct methodology for using Webmail prior to trying to access their Council email using this system.

5. Procedure statement

1. For mobile working, access to Council information, networks and applications (including Derbyshire email) can be attained via the Derbyshire Direct Access facility using Council owned and managed mobile devices (laptop, PC, tablet) that have been used to log directly on to the Council network at the workplace.

2. If a Council mobile device has the relevant credentials (domain certificate, machine name and password, username and password) and therefore the required levels of authorisation to establish the connection, then access to the Council networks, via Derbyshire Direct Access can be attempted using an available Wi-Fi network.

3 It is possible to access some Council resources via the Remote Access Portal and Derbyshire Email is accessible via Microsoft Office Online (by visiting **Microsoft Office 365**). Both these can be achieved from a remote location (such as home) using non-wireless or wireless technology, via an Internet browser on a personal computer, tablet or smartphone. In order to use these resources, Multi-Factor Authentication (MFA) is necessary. This must be done be by registering a mobile phone with the ICT Service desk. A verification code will be sent to that phone when using any of the above applications.

4 Staff should ensure they pick the tick box stating if they are using a private or shared computer according to the rules given on the entry web page. Staff must ensure when using this service that https is displayed at the start of the address line and the padlock symbol is displayed on the browser window. At the end of using the resource, staff must logoff the relevant resource and close the browser window. Failure to do so can leave the account accessible to hackers.

5 Reference and adherence to the ‘Access control policy’ must be maintained by managers when staff are enabled with Council network resources that can be accessed remotely.

6 It is possible to install the Microsoft Outlook app on a remote device (smartphone and/or tablet). This must only be done through a legitimate app store. If at all possible, use of a Council managed remote device should be made available to staff who may need to remotely use email with information classified as controlled/restricted. Extra care must be made to ensure devices with Microsoft Outlook app installed are not shared/used by others (including friends/family) as controlled/restricted information may be lost/stolen. A line manager must be consulted and informed if the Microsoft app is in consideration to be used on a remote device. The Microsoft app must be uninstalled if no longer required.
In order to use this App a, Multi-Factor Authentication (MFA) is necessary. This must be done by registering a mobile phone with the ICT Service desk. A verification code will be sent to that phone when setting up the app.

7 At the end of using the Microsoft Outlook app, staff must close the app and 'lock' the device. Failure to do so can leave the information open to anyone with access to the device.

8 Staff who have the Microsoft Outlook app installed on a remote device must report any misuse, loss or theft of that device to the Service desk.

9 If the mobile phone which is used for MFA is stolen/lost/changed it must be reported to the Service Desk.

10 Connection to the Council's network should only be attempted using the domain logon and password credentials which staff are issued with. Connection using network infrastructure that does not belong to the Council may enable traffic to be viewed, altered or deleted by an attacker.

11 Extra care should be taken to properly close all applications, network connections and web browsers when using PCs, mobile devices and software not officially provided by the Council. Passwords, logon credentials and sensitive files can be left behind on un-trusted devices, making them readily available to subsequent users.

12 If a Wi-Fi connection cannot be made at a site, email can be viewed using the specified Outlook Web Application:
https://outlook.office365.com/owa/derbyshire.gov.uk.

13 Staff using a Wi-Fi system must ensure that the network is as secure as possible. View the "Wi-Fi Security" advice below from the "Information Commissioner's Office" as a guide as to how this can be done but the Council states staff must connect via Wi-Fi WPA2 standard and that they adhere to the Council's Password policy. (See accompanying information concerning 'Wi-Fi security' at the end of this policy)

14 All users accessing Derbyshire networks or specialised external services via mobile devices must abide by the Council's associated security policies and any applicable codes of connection and conduct.

15 Managers are responsible for ensuring that their staff know how to use approved devices and software to connect to and safely/securely use Derbyshire networks.

16 Managers of staff for whom they have responsibility must ensure they have up to date contact and device information for their staff making use of mobile working.

17 Users conducting mobile working should not allow or give permission for unauthorised users (including family and friends) to use that PC/mobile device.

18 Any information concerning passwords, usernames, network credentials or requirements/ability used to access the Council's information and systems by mobile working must not be shared with other staff, unauthorised users, third party vendors, family, friends or members of the public.

19 Mobile devices distributed by the Council should only be used by authorised parties for authorised Council business or purposes in accordance with the Council's Acceptable Use Policy and associated security policies.

20 Adherence to the Council's Safe Haven Guidance is a requirement of mobile working.

21 Users should always be aware of the potential for other people (including family, friends, colleagues and intruders) to overlook screens and keyboards and view personal, confidential information or passwords. Users should check this is not taking place.

22 During short periods of time when devices are not being used (e.g. when on the phone) users should lock PCs and devices to prevent screens being overlooked. For example, on PCs/laptops this can normally be achieved by holding down the ctrl-alt-del keys together and choosing the 'lock computer' option or by holding down the Windows (flag) key and hitting the L key.

23 Users should ensure that all applications are properly closed/logged off, browsers are closed and internet sessions are logged off, prior to network connections being logged off and closed.

24 On completion of work, mobile workers should fully power down or log off remote devices.

25 Active equipment that is unlocked and in use should not be left unattended at any time.

26 A password should be set up and used on all equipment that can be locked by use of a password. For example, mobile devices can be set locked using a password and this facility should not be disabled by the user.

27 Transfer of personal or restricted information must take place through a secure, encrypted channel (identified by the https address prefix and padlock symbol) using agreed software/applications.

28 Person identifiable information and/or business data should not be stored on the PC/mobile device. If possible, data should be accessed from and be stored on Council servers or on password protected and encrypted portable/removable media.

29 Users must not install or update any software on Council owned or managed devices.

30 Users must not install any screen savers on Council owned or managed devices.

31 Users must not download or install any applications or items on Council owned or managed devices from the internet unless authorisation has been gained from the ICT Service Desk. Access to cloud services, even where software is not downloaded, are not permitted without approval.

32 Users must not alter or disable any element of the configuration of devices, including data encryption and anti-virus software.

33 Only Council provided removable media should be used and must be safely 'closed' if necessary and removed from any device when finished with.

34 Person identifiable information and data should only be sent using official channels, authorised software/applications and official equipment deemed fit for the purpose. For example, text messages containing person identifiable information and data should not be sent via mobile phone.

35 Staff entrusted with a Council mobile device are responsible for ensuring that it is regularly connected to the Council network for automatic upgrade of anti-virus software and other software licensing agreements.

36 If it is likely that a device will not be connected to the Council network for a period of greater than 90 days, then that device should be entrusted with a line manager for connection to the network for anti-virus and software licensing upgrade requirements.

37 In the event that a user becomes aware of an information or data breach or accidental disclosure, this matter must be reported immediately via the Council's information security incident reporting procedures: https://staff.derbyshire.gov.uk/information-security/report-a-security-incident/report-a-security-incident.aspx

Wi-Fi Security.
Computers and many other devices, including smart phones can connect to the internet wirelessly using Wi-Fi. An unsecured Wi-Fi connection makes it easier for hackers to access private files and information and it allows strangers to use the internet connection for their own purposes.

These are general tips on changing private router and network settings. Staff may need to check the instructions for their wireless equipment for the technical details. If staff need more guidance on checking or changing settings, the Wi-Fi equipment supplier or internet provider will provide advice on their websites.

How do I check whether my network is secure?
Wi-Fi networks are accessed through a physical device called a router – also known as a hub. Staff will need to connect to their router to check its network settings. To do this, staff will need the router's IP address, username and password. Open the browser and enter the router's IP address into the address bar. When asked, enter

username and password. The router settings will allow staff to find out whether the connection is already secured and will let a more secure password be chosen.

How do I secure my network?
The following tips will help staff to use Wi-Fi more securely and to protect personal information.

Change the wireless network's default name
A Service Set Identifier (SSID) is a unique ID used for naming wireless networks and ensures the network name is different to other nearby networks. Staff should change the network name from the router's default. This will make it harder for anyone to identify the browser and guess its default settings.

Use encryption
Encryption scrambles messages sent over wireless networks so that they cannot be read easily. If the network is not encrypted, then staff should enable encryption on their settings page. There are different forms of encryption, but the Council requires that staff use the Wi-Fi Protected Access (WPA/WPA2) version because it is stronger than other versions such as Wired Equivalent Privacy (WEP). (Derbyshire County Council requires that staff must use WPA2).

Choose a strong password
Change the password from a default supplied with the router. Make sure the password is easy to remember but would be difficult for a stranger to guess and preferably something with a combination of letters and numbers. Avoid using something obvious such as street name. (Derbyshire County Council requires staff to follow its Password Policy)

Hide the network ID
A router broadcasts its SSID to anyone within range. When the option is available staff should alter the router settings to not broadcast the SSID and therefore avoid alerting hackers to the network's existence.

Check that the device does not auto-connect to Wi-Fi signals
If the device is set to automatically connect to available Wi-Fi networks, then staff run the risk of automatically connecting to unknown and potentially dangerous networks. Staff should switch off auto-connect on the device settings page – refer to the manufacturer's instructions for more details.
http://ico.org.uk/for_the_public/topic_specific_guides/online/wifi_security