Desktop and Mobile Device Procedures

1 Version History details and author

1.0	27/10/2010	Completed for Distribution	Jo White
1.0	24/11/2010	Approved by Information Governance Group	Jo White
2.0	20/12/2011	Reviewed by Information Governance Group	Jo White
3.0	25/01/2013	Reviewed by Information Governance Group	Jo White
4.0	10/02/2014	Reviewed by Information Governance Group	Jo White
5.0	13/04/2015	Reviewed by Information Governance Group. 'Desktop PC Security Procedures' and 'Laptop & Mobile Device Security Procedures' combined to form this document. Version control continued.	Jo White
6.0	09/05/2016	Reviewed by Information Governance Group.	Jo White
7.0	12/06/2017	Reviewed by Information Governance Group. Transformation changed to ICT.	Jo White
8.0	09/07/2018	Reviewed by Information Governance Group. Apple and Android operating systems added.	Jo White
9.0	06/08/2019	Reviewed by Information Governance Group. PC Commissioning unit changed to ICT Asset Team. Dual booting removed. Clarification around email configured on DCC smartphones.	Jo White
10.0	08/09/2020	Reviewed by Information Governance Group. Removal of old Windows OS.	Jo White
11.0	05/10/2021	Reviewed by Information Governance Group.	Jo White
12.0	04/10/2022	Approved by Information Governance Group. No changes.	Jo White
13.0	14/11/2023	Approved by Information Governance Group. No changes.	Jo White
14.0	10/12/2024	Approved by Information Governance Group. Reference to Windows 10 removed. Reference to BYOD added. Agency staff added. Bluetooth evaluation removed.	Jo Williams

This document has been prepared using the following ISO27001:2022 standard controls as reference:

ISO Control A.5.9 - Inventory of Information and other associated assets
ISO Control A.5.10 – Acceptable use of Information and other associated assets
ISO Control A.5.18 – Access Rights
ISO Control A.5.17 - Authentication information
ISO Control A.5.36 - Compliance with policies, rules and standards for information security
ISO Control A.5.37 - Documented operating procedures
ISO Control A.7.5 – Protecting against physical and environmental threats
ISO Control A.7.7 - Clear desk and clear screen
ISO Control A.7.8 - Equipment siting and protection
ISO Control A.8.1 – User endpoint devices
ISO Control A.8.2 – Privileged access rights
ISO Control A.8.5 - Secure authentication
ISO Control A.8.7 - Protection against malware
ISO Control A.8.8 – Management of technical vulnerabilities
ISO Control A.8.18 - Use of privileged utility programs

2 Introduction

Derbyshire County Council is reliant on the use of ICT equipment across all areas of the authority. Desktop, laptop and mobile computing devices are provided for use by those who require them to carry out their duties. Devices are also made available for use to members of the public for access to information, resources and Council services. The Council and its employees have a duty to ensure that appropriate levels of security are applied to all computing devices.

The purpose of these procedures is to ensure that all computing devices – both desktop and mobile, are used, configured and managed in a secure and safe way and to identify and describe the steps required to achieve and maintain this.

Desktop computing generally refers to computers which can be used in an office environment over long periods and has historically referred to computers identified as 'static' or 'fixed' with a base unit, keyboard, mouse and monitor. Laptops and tablets are now used more widely in offices across the Council and cannot be treated solely as mobile devices. These procedures will treat laptop and tablet computers as both 'desktop' and 'mobile' computing devices.

Mobile computing is typically associated with devices which are easy to carry, relatively small, compact, run predominately on battery power and allow for access to the internet and general computing capability including components which may enable interconnection between the mobile device and the office/desktop environment.

3 Desktop Computing Procedures

ICT equipment such as desktop, laptop and tablet computers are all capable of being used in the office environment over long periods on a daily basis.
Operating systems such as Apple IOS and Android are in use across the Council on various devices, however, this procedure primarily covers the support and configuration of the Council's main Windows operating system estate.

The scope of these procedures cover:-

- All desktop, computing devices provided by the Council and configured with a Windows operating system image
- Computing devices which are predominantly used in an office environment
- Computing devices which are, or can be, connected to the Council's computer network.

Access to all desktop computing devices must be controlled using secure methods and procedures in order to prevent damage to Council assets and reputation.

<u>DESKTOP COMPUTING CONFIGURATION</u>

Normal, everyday use of desktop computing devices provided by the Council for use within an office environment requires the following configuration and security considerations:

All Council desktop computing devices are supplied to users with a preconfigured standard Windows Operating System image which Digital Services has developed. Differing departmental requirements result in department specific applications being layered on top of the standard image. In terms of security, all desktop computing devices connected to the Council's Derbyshire network domain will have the same level of security applied across all areas.
All Council desktop computing devices are subject to the following configuration which ensures they are added to the Council network and have the correct security configuration settings applied:

- All Council desktop computing devices use the Microsoft Windows family Operating System.
- New desktop computing devices will have the approved "standard" Windows image loaded from Microsoft System Configuration Manager by the Digital Services Asset Management Team. The configuration of the desktop image deals primarily with the "look and feel" of Windows and some changes which may be necessary for optimisation of the operating system.
- All newly purchased desktop computing devices come with on-board TPM (Trusted Platform Module) chips which allow full disk hardware encryption and encryption policies are enforced at the point of the installation of the Windows operating system by the Configuration Manager software.
- Desktop computing devices can only be added to the Council's computer network (Derbyshire Domain) by an authorised Digital Services account that has sufficient access permissions to do so. This is typically achieved as part of the Windows installation 'imaging' process by the Configuration Manager account but in exceptional circumstances, can also be completed manually by authorised personnel.
- Newly commissioned desktop computing devices are added to the Derbyshire Domain using an asset tag number with a prefix relevant to the type of computing device e.g. **WS** for 'static' computers, **WL** for laptops and **WT** for tablets: e.g. a new laptop with asset number: **123456** will have the laptop account name: **WL-123456.**
- Council desktop computing devices are protected from viruses and spyware/malware using System Centre Endpoint Encryption, Virus definition files will be released across the network automatically when they become available from Microsoft.
- Users are not able to install un-approved software, even for a trial or demonstration. Any request for the installation of new software must be raised with the Service Desk.
- Once a desktop computing device has been added to the Domain, the security settings for the device are applied and enforced automatically, immediately on "boot-up" of the computer. These security settings are applied and enforced at the Domain level using Windows Group Policy which will override any changes made locally on the device.
- The locally Built-in administrative passwords on desktop computing devices are changed automatically by Group Policy (on boot-up) once added to the Domain.
- The locally Built-in Administrative groups on desktop computing devices are propagated by all the relevant Digital Services network groups and users who require admin privileges e.g. Area Support, Support Desk etc – including some departmental network groups which have been approved and authorised to be added.

- Users who have an account within at least one of the groups added to the local administrator's group will be provided with full administrative control of the computer but will not be able to override the settings which have been applied by Group Policy.
- Screen savers and the desktop 'look and feel' will be supplied and approved by the Digital Services team and cannot be changed by users. Under no circumstances should software be installed to simulate user activity which disables the screen saver lock functionality following a period of inactivity.
- Any desktop computing device which has not been used for 90 days or more will have its computer account disabled and then removed from the network - which will mean it can no longer be used. The Digital Services Service desk will need to be contacted in order to re-establish the device on the Council computer network if necessary.

N.B Desktop computing devices which have not been provided by the Council but have been approved for use will be subject to the relevant security checks and procedures by Digital Services before being considered for connection to the Council's computer network.

4 Mobile Computing Procedures

The proliferation of mobile computing devices has facilitated increased flexibility and mobile working for the Council. These procedures aim to cover the security of mobile computing devices which are currently in use across the Council.

N.B - Please note that smart phones, although covered here in terms of mobile computing, involve other aspects of use which are covered in the Council's Mobile Phone Usage policy and BYOD policy.

MOBILE COMPUTING CONFIGURATION

For the purpose of these procedures, devices which can be categorised as mobile devices include; Laptops, tablets and smart phones and require the following considerations:

- Mobile computing devices which do not satisfy the hardware and/or minimum software (Operating System) installation specification should not be used to run Council applications nor should any attempts be made to use or bypass application/system authentication processes or controls when using such devices.
- Connecting any mobile computing device to the Council network must be evaluated by Digital Services and subject to existing Council configuration standards and procedures and Digital Services must be contacted for the approval or configuration of any of these devices whether the connection is to be made wirelessly or wired.
- All mobile/smart phone type devices (excluding laptops or tablets) issued by the Council, must only be used for Council business and used as a communications and "resource" tool – providing and acting as an enabler to access information from the Council Website, intranet and other web-based information and resource web sites in line with the Council's Internet, E-mail and Social Media Acceptable Use Policy.

- Wireless based technology is treated in accordance with the Council's Wireless Network Policy.
- Email is configured on all DCC smart phones and there is a service request that can be used to enable DCC email on personal phones with an MFA token.
- Near field communication (close proximity communication) between devices such as smart phones, should not be activated.
- Mobile computing devices should only be connected to other Council issued devices or equipment which have been configured by Digital Services.
- Mobile devices such as smart phones should only be used with applications, software and facilities supplied with the device. Official Council prescribed procedures and methodologies of working, such as the use of OWA and push email, should not be circumvented.
- The downloading and use of software, facilities, programs and apps on mobile computing devices is not permitted unless the software has already been approved by the Council.
- Security measures installed on any mobile computing device should not be circumvented, altered or deleted.
- Any multimedia memory cards (e.g. SD cards) fitted to a mobile computing device and permitted for the storage of Council data (including photographs, sound files etc…) must be encrypted.

LOCATION

Desktop and mobile computing devices which are used by Council employees, elected members, partner agencies, agency staff, contractors and vendors are located across many sites and buildings.
The wide nature of access to many of these buildings and locations requires increased vigilance and awareness of the need for desktop and mobile computing devices to be secure and protected from unauthorised access, theft, physical damage and tampering.

Care and professional judgement to protect information and data should be taken when locating desktop and mobile computing devices to ensure that, wherever possible, the risk of the following is reduced:

- Display screen/s may be visible to members of the public/service users.
- There is a danger of physical damage to a device e.g. dropping, water, electrical.
- Devices may be subject to interference e.g. strong electromagnetic sources.
- Devices may easily be picked-up and/or stolen in obscured, low visible, non-staffed areas.

It is important to observe and maintain the physical security of rooms and offices where desktop and mobile computing devices are located.

USE

Desktop and mobile computing devices may 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.
All users of Council desktop and mobile computing devices must ensure at all times that:

- Account logon and system passwords are kept private and **not shared**, **displayed** or **communicated** to anyone else.
- Sensitive and personal data is not stored on any desktop or mobile computing device, hard drive or any portable memory devices - in the event of the Council network being unavailable, any data which may have been temporarily stored must be transferred to the Council network and removed from the device as soon as possible.
- Data and Information saved to storage devices such as SD card/USB sticks via a desktop computing or mobile device must only be copied to an authorised portable device which is encrypted in accordance with the Council's Encryption Policy and must only be stored temporarily on the device before being transferred to the Council's computer network.
- Display screens on desktop and mobile computing devices must be locked by users when away from the device.
- Unauthorised, non-standard equipment such as personal mobile phones or personal USB memory devices are not connected or inserted into any desktop or mobile computing device.
- Software is not installed on any desktop or mobile computing device by unauthorised staff – any software installed must be (or going through the process of being) placed on the approved software list
- Desktop and mobile computing devices must not be mishandled, wilfully damaged or tampered with in any way – this includes taking off the cases, covers or removing of any screws and/or fixings.
- Any suspicious or unknown equipment near or around desktop and mobile computing devices should be reported immediately to a senior manager and Digital Services.
- All desktop and mobile computing devices are logged off and shut down when not in use for an extended period (i.e. overnight) with display screens powered off.

Please note:
Any warnings visible on screen from the Microsoft System Centre Endpoint Encryption software about identified/detected threats from viruses/malware must be reported to the Digital Services Service Desk as soon as possible.

COMMISSIONING AND REPLACEMENT:

- All requests for the purchasing of new desktop and mobile computing devices must be placed through Digital Services except for a few exceptions e.g. schools, specialist educational equipment.
- Every new desktop and mobile computing device ordered from the Council's approved supplier must be provided with a Council asset tag number. This number is used to name the device and is used as an inventory tag by the Service Desk to record fault calls or installation/maintenance requests.
- Except where a workplace assessment or business need dictates otherwise, IT equipment including desktop and mobile devices are replaced using the

'standard' approved hardware and software specification as on the current approved software and hardware list maintained by Digital Services.
- The device asset number is recorded in the central hardware inventory database. The life of the device from commissioning to disposal can be tracked and recorded.

MAINTENANCE

- All desktop and mobile computing device maintenance whether routine or major is carried out by Digital Services authorised staff or the Council's authorised third parties.
- Only staff working within an ICT function (or persons authorised by Digital Services) may perform maintenance, install applications/software or make system configuration changes to desktop and mobile computing devices. Staff may occasionally be requested to assist while under the supervision and authorisation of Digital Services as appropriate.
- A standard base configuration is installed on all Council desktop and mobile computing devices. Any variations and additions must be agreed by Digital Services and the Information Security Manager
- Desktop and mobile computing devices are protected against malicious code in accordance with the authority's Malicious software and anti-virus Procedure
- Desktop and mobile computing devices will be maintained in accordance with all relevant Council policies and procedures

Council employees, elected members, partner agencies, volunteers, agency staff, third parties and vendors must be mindful of the potential for unauthorised access and viewing of Council data and Information by members of the public/service users and take appropriate steps to avoid or prevent this in line with the Council's Safe Haven Guidance.

DISPOSAL

All desktop and mobile computing devices are subject to the Council's ICT Disposal Procedures.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.