Remote and Home Working Policy

Signed: Claire Hamilton Chief Executive.

Remote and Home Working Policy

1. Introduction – Remote and Home working

Purpose

Dacorum Borough Council provides users with the facilities to work at home and/or remotely (i.e. remote DBC Offices) as appropriate. The Council will ensure that all users who work remotely / home are aware of the acceptable use of both portable and static computer devices and remote / home working opportunities.

The purpose of this policy is to protect the Council's information systems, manage information risk and reduce it to an acceptable level, while facilitating reasonable use of information in supporting normal business activity and that of our partners.

This Policy provides direction for personnel when working from home or remotely using mobile or static computer equipment to enforce compliance with acceptable working standards and practices.

2. Policy Governance and Strategy

In line with Dacorum Borough Council (DBC) strategy, this policy document supports the use of technology as a business enabler whilst maintaining flexibility, confidentiality, integrity and availability.

DBC is making ever increasing use of remote and home working technology, and this policy forms a subset of the Council's other policy documents, and therefore will be used in conjunction all other Council policies.

In order to strike this balance DBC maintains a set of information security management and technology policies and procedures of which this document is one.

The complete list of information security policies can be found in the Intranet, under Resources>Document Centre>Information Management and Security.

2.1. Users must read and understand the ICT Security and Data Protection policies and procedures and to exercise good judgment when processing the Council's information, using information systems and seek advice from their line manager or Information Team Leader if they have any queries in respect of any of the Council's ICT, Data Protection, Information Security, Remote Working Policies.

2.2. Information systems and technology are an important asset. Dacorum Borough Council (the Council) are committed to preserving the confidentiality, integrity, and availability of our information assets;

- For sound decision making;
- To deliver quality services;
- To comply with the law;

- To meet the expectations of our customers;
- To protect our reputation as a professional and trustworthy organisation.

3. Scope

3.1. This policy applies to all councillors, employees, temporary staff, partners, contractors and agents of the Council (i.e. voluntary sector) who use or have access to council information, computer equipment or ICT facilities.

3.2. ICT Hardware /Devices includes, but is not limited to: desktop PCs, Laptops, Tablets, mobile phones, smartphones, network cabling, routers, firewalls, switches, hubs, printers, removable storage devices, digital cameras and other peripheral devices, owned by the Council or 3rd Party accredited and authorised devices. Also known as "Council owned devices."

3.3. ICT Software includes, but is not limited to: operating systems and bespoke or supplier software / applications running on any of the above hardware, web applications, apps, remote apps, collaboration, meeting and video conferencing, files on network shares and other solutions hosted on premise, shared premise or Cloud by the Council's ICT Department or by 3rd parties.

3.4. ICT Databases includes, but is not limited to: Local and Network databases, SQL Databases, Oracle Databases, Web Databases, Geographical Mapping, Datasets, hosted on premise, shared premise or Cloud by the Council's ICT Department or by 3rd parties.

4. Policy Compliance and Disciplinary Action

4.1. All employees, councillors and anyone who delivers services on the Council's behalf e.g. contractors, partners, agents or other third parties with access to the Council's information assets have a responsibility to comply with this policy and promptly report any suspected, potential or observed security breach;

4.2. ALL BREACHES MUST BE REPORTED TO THE COUNCIL'S INFORMATION SECURITY TEAM LEADER IN THE FIRST INSTANCE. FURTHER DETAILS ARE PROVIDED IN THE 'Personal Data Breach or Incident Reporting Procedure' (DBC999 IS Proc) found here.

4.3. Security breaches that result from a deliberate act or omission or from an otherwise negligent disregard of any of the Council's Information Security and Information Management policies and/or associated procedures may result in disciplinary action being taken against the employee under their contract of employment or, in the case of a councillor, under the Members' Code of Conduct. In the event that breaches arise from a deliberate or negligent disregard for the Council's polices and/or procedures, by a user who is not a direct employee of the Council, or a councillor, the Council may take such punitive action against that user and/or their employer as the Council deems appropriate.

4.4. The Council may refer the matter of any breach of the Council's Information Security and Information Management policies and/or associated procedures to the police for investigation and (if appropriate) the institution of criminal proceedings if in the reasonable opinion of the Council such breach has or is likely to lead to the commissioning of a criminal offence.

4.5. If you do not understand the implications of this policy, any of the policies referred to within it or how the policies may apply to you, please seek advice from your line manager, ICT or Information Security Team Leader.

4.6. In the event of an apparent breach of the policies, by a user, a group of users, the ICT department has authority to withdraw access temporarily or permanently to all or any subset of ICT facilities, including but not limited to;

4.6.1. Network (Active Directory)
4.6.2. Emails and Internet
4.6.3. ICT Business Systems
4.6.4. Remote Access Systems

4.7. In the event of an apparent breach of the policies, by a user, a group of users, the ICT department has authority to seize and quarantine any ICT equipment and peripherals as part of any investigation into user(s) activities.

5. Policy Statement

5.1. Any user accessing the Council network and any product in the scope cited in clause 3 above and/or PSN (formerly GCSx) services or facilities, or processing OFFICIAL information, **must only use a Council owned authorised and managed device** which has appropriate technical security and advanced authentication mechanisms in place. For definitions of OFFICIAL – please see Appendix 1 of this policy.

5.2. Users must complete a health and safety review of the home or remote access area and have authorisation from their line manager before being allowed to work remotely or at home

5.3. Users must take all reasonable steps, due care and protection of Council owned devices at home / remote locations or when moving between home, office, and any other remote locations to ensure they are not misplaced or stolen. **DO NOT LEAVE THE LAPTOP UNATTENDED OR IN A PLACE WHERE THEFT COULD OCCUR, i.e. IN A CAR OR ON PUBLIC TRANSPORT**.

5.4. Users will not install or update any software, install screen savers, store personal files, or change the configuration of a Council owned device.

5.5. Users must allow the updating remotely or at work site of the Council's Anti-Virus software, and any relevant vendor patches.

5.6. All Council owned devices in the scope defined above must have an asset tag; users must not deface or remove the asset tag number.

5.7. All faults with the Council owned devices must be reported to the ICT helpdesk.

5.8. All Council data [OFFICIAL OR OFFICIAL SENSITIVE] should be stored and accessed centrally (on the network) wherever possible. The Councils ICT Service will provide a secure access mechanism to all home / remote users. Personal Data or Special Category Data **MUST NOT** be stored on the local drives of the Council owned device – this includes the Documents/My Documents folder and the desktop.

5.9. Laptops, (home or remote) routers must be encrypted and routinely checked updated. USB Memory Sticks must not be plugged into Council owned devices for any purpose with the sole exception of those authorised to access the Council's Business Continuity Plan and Emergency Plan using encrypted USB Sticks.

5.10. OFFICIAL or OFFICIAL-SENSITIVE information **MUST NOT** be e-mailed from a Council email account to a private / home email account or any non-work email account.

5.11. Under no circumstances should the Out of Office message direct people to a private non-Council email address

5.12. No family members may use the Council owned devices. The equipment is supplied for the staff/members' (or anyone in the scope of section 3.1 of this policy) sole use.

5.13. The user must take reasonable care of the ICT equipment supplied. Where any fault in the equipment has occurred due to accidental damage, the user must report this to the ICT department, and the Council's insurance officer.

5.14. Under no circumstances should Personal or OFFICIAL information printed to a home printer (wired or wirelessly). Staff can use Print to pdf and email using Council email accounts. Under extremely exceptional circumstances (Emergency Plan or Critical Incident) this can be authorised by an Assistant Director or above (see 5.15), for the duration of the incident; any such documents should be limited to the operation of the plan or management of the incident and should not contain Personal Data.

5.15. Printing from home or taking copy of documents or originals (leases etc.) home, must be on an exceptional basis, and the authorisation form must state the risks, and the employee's understanding and acceptance of such. The requirement will be time bound and removed when no longer required. The form (DBC701 ISF) must be signed off by the appropriate director or assistant director.

5.16. Paper documents containing OFFICIAL information must be locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing OFFICIAL information must destroyed securely after use by using cross-cut shredders or the Council's secure loop confidential waste bins.

5.17. Microsoft Teams can be used to share documents externally with partners, contractors who will receive a timed linked invitation. Teams project groups should avoid sharing personal data wherever possible unless approved and authorised, and should not share any other documents other than those related to the project.

5.18. When the project has been completed, consideration must be given to the revoking of Teams access to external partners and deletion or removal of the previously shared documents.

5.19. Teams audio or video conversations should be conducted where conversations cannot be overheard by unauthorised individuals or external parties

5.20. Teams recordings must only be recorded with the consent of all participants. The recording should only be made available to meeting participants, and deleted once the minutes have been approved.

5.21. Teams Chat should be deleted when no longer required and in any even kept no longer than one month.

5.22. When attending formal Teams Meetings, Council or Committee meetings use the approved corporate backgrounds only.

5.23. It is recommended that the home user brings in the device to the office from time to time, to ensure that any updates and patches are downloaded to the device.

6. Roles and Responsibilities

6.1. The Assistant Director (Corporate and Contracted Services) holds the appointment of SIRO. The Council's Senior Information Risk Officer (SIRO) has responsibility for managing information risk on behalf of the Senior Leadership Team (SLT), setting strategic direction and ensuring policies and processes are in place for the safe management of information.

6.2. Directors have responsibility for understanding and addressing information risk within their directorate, assigning ownership to Information Asset/System Owners and ensuring that within their directorate appropriate arrangements are in place to manage information risk, and to provide assurance on the security and use of those assets.

6.3. Information Asset/System Owners undertake information risk assessment, implement appropriate controls, recognise actual or potential security incidents and ensure that policies and procedures are followed

6.4. The Information Security Team Leader is responsible for providing, information security advice, and support to all staff, develops appropriate information security, management and technology policies to protect the Council's information, promotes information security awareness, guidance and alerts, attends the relevant forums and best practice groups on information security matters, provides information security training

6.5. ICT are responsible for being the custodian of Council-owned devices, the local area network, wide area network, servers in its remit, implementing and administering the appropriate technical security controls.

6.6. ALL USERS – Information Security is everyone's responsibility and all employees, members, third parties and partners who have access to the Council's information are required to comply with this policy and supporting policies, standards and procedures.

7. Other Supporting Information Security, Management and Technology procedures.

7.1. This policy is supported by more detailed policies, standards and procedures; these include but are not limited to the following

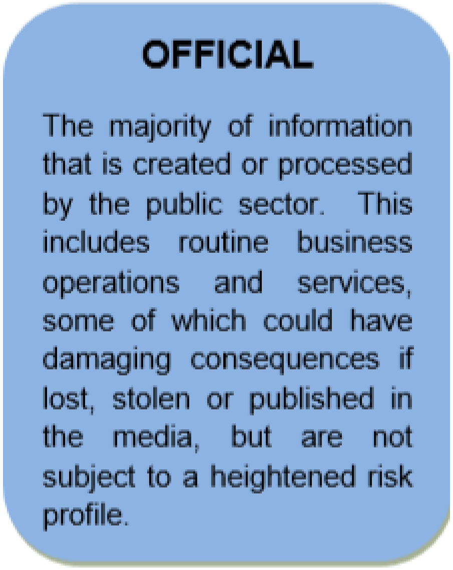
7.1.1. DBC001 IS Corporate Information Security Management Policy
7.1.2. DBC010 IS Corporate Information Technology Security Policy
7.1.3. DBC900 IS Information Security Incident Reporting Policy
7.1.4. DBC999 IS Proc – Personal Data Breach or Incident Reporting Procedure
7.1.5. DBC100 IM GDPR / UK Data Protection Act Policy
7.1.6. DBC701 ISF – Authorisation to have manual records at home

8. Review of the Remote and Home working Policy

8.1. The current version of this policy will be held on the Council's Intranet along with information that supports this policy.

8.2. This policy and all supporting procedures will be reviewed at appropriate intervals but no less frequently than every 12 months.

Appendix 1 – OFFICIAL (and OFFICIAL Sensitive) Information[1]



OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened risk profile.

The typical threat profile for the OFFICIAL classification is broadly similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend UK Government data or services against compromise by attackers with bounded capabilities and resources. This may include (but is not limited to) hacktivists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.

OFFICIAL
Definition: ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level.

This includes a wide range of information, of differing value and sensitivity, which needs to be defended against the threat profile described above, and to comply with legal, regulatory and international obligations. This includes:

- The day to day business of government, service delivery and public finances
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under Data Protection legislation, GDPR or other legislation (e.g. Local Government Act).

Baseline Security Outcomes:

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

- ALL HMG information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them in line with local business processes.
- Baseline security controls reflect commercial good practice

Marking:

There is no requirement to explicitly mark routine OFFICIAL information.
Baseline security measures should be enforced through local business processes.

A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE'

Data Owners are responsible for identifying any sensitive information within this category and for putting in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements. Individuals should be encouraged to exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate

To support specific business requirements and compartmentalise information, organisations may apply an optional DESCRIPTOR, alongside the OFFICIAL-SENSITIVE classification marking, to distinguish particular types of information and indicate the need for additional common sense precautions to limit access.

Please also refer to the following documents;

OFFICIAL Information FAQ's

and

Working with Personal Information

Revision History

Author:	John Worts - Information Security Manager
Owner:	Mark Brookes – Assistant Director (Corporate and Contracted Services)
Current Version	2.1
Full Document Title	DBC700 IS Policy – Remote and Home Working Policy

Revision Date	Previous Revision Date	Previous Version	Summary of Changes	Next Review Date
20th June 2012	n/a	n/a	New document to be included as part of IA document structure	June 2013
11th July 2012	20/6/12	0.1	Approved FINAL	July 2013
2nd August 2013	11/7/12	1.0	Changes to 5.3 re personal files and 5.6 regarding USB	-
6th December 2013	2/8/13	1.1	Changes to reflect PSN	-
3rd April 2014	6/12/13	1.2	USB Memory Policy. Minor spelling mistakes corrected.	April 2014
31st December 2014	3/4/14	1.3	Update on storage of Cryptocard	December 2015
4th April 2016	31/12/14	1.4	Section 5.12 sole use statement amended to include all in policy scope	April 2017
23rd October 2017	4/4/16	1.5	Statement about storage of data on local drives. Change to document owner (MB)	October 2017
25th May 2018	23/10/17	1.6	GDPR / Data Protection Act 2018	May 2019
5th August 2019	25/05/18	1.7	Reflects structure	August 2020
13th August 2020	5/8/19	1.8	5.15 (Printing) clause added. Overhaul of GPMS to new schema (OFFICIAL and OFFICIAL-SENSITIVE) including references to GOV.UK GPMS schemes. Removed 5.4 (Obsolete reference to Cryptocard). Changes to reflect Intranet locations. Use of prescriptive language. Minor edits to enhance grammar. Removed duplicate entries.	August 2021
16th September 2020	13/8/20	1.9	Added in Meetings / Recording Software in scope	September 2021
3rd May 2022	16/9/20	2.0	Replaced CMT with SLT, updated network shares as in scope, updated outdated hyperlinks and new clauses in section 5 added.	May 2023

Document Approvals

Version	Approved By	Date
2.1	Legal Governance	May 2022