Remote and Home Working Policy

Signed: **Chief Executive.**

Number:	**DBC700 IS Policy**	**Title:**	**Remote and Home working Policy**				
Owner:	**AD – Legal, Democratic & Regulatory**	**Rev**	**1.8**	**Date**	**5th August 2019**	**Classification**	**UNRESTRICTED**

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 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 Information Management and Security….Policies.

2.1. Users are also encouraged to be familiar with the ICT policies and procedures and to exercise their good judgment when using The Council's information and information systems and seek advice from their line manager or Information Security Manager if they have any doubt about what would be appropriate.

2.2. Information systems and technology is 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, 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. IT 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 Parties accredited devices.

3.3. IT Software includes, but is not limited to: operating systems and applications running on any of the above hardware, web applications and solutions hosted either internally or by 3rd parties.

3.4. IT Databases includes, but is not limited to: Local and Network databases, SQL Databases, Oracle Databases, Web Databases, Geographical Mapping, Datasets, hosted internally or run 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 promptly report any suspected, potential or observed security breach;

4.2. ALL BREACHES MUST BE REPORTED TO THE COUNCIL'S INFORMATION SECURITY OFFICER IN THE FIRST INSTANCE – FURTHER DETAILS ARE PROVIDED IN THE 'Personal Data Breach or Incident Reporting Procedure' (DBC999 IS Proc) found on the Council's Intranet.

4.3. Security breaches that result from a deliberate act or omission or from an otherwise negligent disregard of any of the Council's security policies and/or 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 security policies and/or 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 Manager.

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/or PSN (formerly GCSx) services or facilities, or processing PROTECT or RESTRICTED information, **must only use a Council owned Managed Device** which has appropriate technical security and advanced authentication mechanisms in place.

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 due care and attention of portable computer devices when moving between home, any other business or other sites. **DO NOT LEAVE THE LAPTOP UNATTENDED, IN A CAR OR ON PUBLIC TRANSPORT**.

5.4. Users must make every effort not to store the Cryptocard token with the laptop, when not in use. e.g NOT kept in the laptop bag overnight.

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

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

5.7. All Council data 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. Data **must NOT** be stored on the C: drive – this includes the Documents/My Documents folder and the desktop.

5.8. Laptops, routers and portable USB devices must be encrypted. USB devices must NOT contain Personal or Sensitive Personal data, and routinely checked for currency. USB Memory Sticks must not be plugged into Council managed devices for any purpose with the sole exception of the Council's Business Continuity Plan and Emergency Plan.

5.9. Confidential or Restricted information must not be e-mailed to / from a home email account.

5.10. All portable computer devices must have an asset tag; users must not deface or remove the asset tag number.

5.11. All faults with the Council owned portable computer device must be reported to the ICT helpdesk.

5.12. No family members may use the portable computer device. 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. The user must take all reasonable steps to ensure the portable computer device, is not misplaced or stolen. The device must not be left unattended or left in a place where a theft could occur i.e. Car.

5.15. Under no circumstances should Personal or RESTRICTED information be e-mailed to a private non-Council email address. For definitions of RESTRICTED and PROTECT – please see section 9 of this policy.

5.16. Paper documents containing RESTRICTED or PROTECT 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 RESTRICTED or PROTECT information must destroyed securely after use.

6. Roles and Responsibilities

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

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 responsible for being the custodian of electronic information 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. DBC170 IS Policy Government Connect (GCSx) Acceptable Use Policy

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 (SharePoint) 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.

9. Definitions Table

Business Impact Level 0 (BIL0) - NO IMPACT

- Not likely to cause any specific loss but may cause some embarrassment if information were to fall into the wrong hands

Business Impact Level 1 (BIL1) - UNCLASSIFIED or NON PROTECTIVELY MARKED assets

- To cause a Financial Loss to the Public Sector of up to £1,000.00
- Likely to cause a Minor Financial Loss to any party - for example under £100.00 for an Individual or Sole Trader or up to £1,000.00 for a Larger Business

Business Impact Level 2 (BIL2) - Criteria for assessing PROTECT assets:

- Likely to cause distress to individuals
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Breach statutory restrictions on the disclosure of information
- Cause financial loss or loss of earning potential, or to facilitate improper gain
- Unfair advantage for individuals or companies
- Prejudice the investigation or facilitate the commission of crime
- Disadvantage government in commercial or policy negotiations with others
- Likely to cause inconvenience or loss to an individual or
- Would undermine the Financial Viability to UK SME's (Small and Medium sized Enterprises)
- Can potentially cause a Financial Loss to the Public Sector of up to £10,000.00
- Likely to cause a Moderate Financial Loss to any party - for example under £1,000.00 for an Individual or Sole Trader or under £10,000.00 for a Larger Business

Business Impact Level 3 (BIL3) - Criteria for assessing RESTRICTED assets:

- Affect Diplomatic relations adversely
- Cause substantial distress to individuals
- Make it more difficult to maintain the operational effectiveness or security of United Kingdom or Allied forces
- Cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or Companies
- Prejudice the investigation or facilitate the commission of crime
- Breach proper undertaking to maintain confidence of information provided by 3rd parties
- Impede the effective development or operation of government policies
- To breach statutory restrictions on disclosure of information
- Disadvantage government in commercial or policy negotiations with others
- Undermine the proper management of the public sector and its operations
- Likely to cause a risk to an Individuals Safety and Liberty

- Would undermine the Financial Viability of a Minor UK based or UK owned Organisation
- Can potentially cause a financial loss to HMG/Public Sector of up to £1million
- Likely to cause a Significant Financial Loss to any party - for example under £10,000.00 for an Individual or Sole Trader or under £100,000.00 for a Larger Business

Revision History

Author:	John Worts - Information Security Manager
Owner:	Mark Brookes – Assistant Director (Corporate and Contracted Services)
Current Version	1.8
Full Document Title	DBC700 IS Policy – Remote and Home Working Policy

Revision Date	Previous Revision Date	Previous Revision Level	Summary of Changes	Changes Marked	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

Distribution List:

Name	Title	Date of Issue	Version
All			

Document Approvals

Version	Approved By	Date
1.8	Legal Governance	August 2019