Corporate Information Technology Security Policy

Signed: **Chief Executive.**

Contents

1. Definition of Information Technology .... Page 3
2. Policy Governance and Strategy .... Page 3
3. Scope .... Page 4
4. Policy Compliance and Disciplinary Action .... Page 4
5. Policy Statements .... Page 5
    5.1. ICT Access Policy .... Page 5
        5.1.1. Password Policy .... Page 6
    5.2. Computer Usage Policy .... Page 6
    5.3. Internet Usage Policy .... Page 8
    5.4. Email Policy .... Page 9
        5.4.1. Negligent Virus Transmission .... Page 10
        5.4.2. Junk Email .... Page 10
    5.5. Malicious Code and Anti-Virus Policy .... Page 11
    5.6. Asset Management Policy .... Page 12
    5.7. Telephone / Fax and Desk Policy .... Page 12
        5.7.1. Telephones .... Page 12
        5.7.2. Fax Policy .... Page 13
        5.7.3. Clear Desk Policy .... Page 13
    5.8. Social Media Policy .... Page 14
6. Roles and Responsibilities .... Page 14
7. Other Supporting Documents .... Page 14
8. Review .... Page 15
9. Document Control .... Page 16

1. Definition of Information Technology

Information (and Communications) Technology (ICT) covers any product, software, application, device, databasethat will store, retrieve, manipulate, transmit or receive information electronically in a digital form. For example, personal computers, removable USB drives, email and network shares.

ICT is concerned with the storage, retrieval, manipulation, transmission or receipt of digital data. Importantly, it is also concerned with the way these different uses can work with each other.

Information at rest in digital storage and devices, or information in transit i.e. sending an email needs to be processed and accessed securely. There are inherent security risks associated with digital information, and technological, physical and organisational controls need to be applied in order to secure digital information, and consequently ensuring the confidentiality, integrity and availability.

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 Information and Communication Technology (ICT) in its collection, maintenance and application of customer information held by DBC and other public sector organisations. The information DBC holds, processes, maintains and shares with other organisations is an important and highly valued asset. Like other important business assets, DBC endeavours to strike the best possible balance between enabling ease and flexibility of use whilst ensuring its information technology and information systems are used appropriately.

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.

The ICT policies are based on industry good practice and, amongst other things, are intended to satisfy the requirements set out by the Information Commissioner, ISO27001 / ISO27002, Government Connect Secure Extranet (GCSX) Code of Connection (CoCo), Payment Card Industry Data Security Standard (PCI/DSS) and Internal Audit Reports.

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. The purpose of the Information Technology Security 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

2.3. 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 includes, but is not limited to: desktop PCs, Laptops, Tablet devices, network cabling, routers, firewalls, switches, hubs, mobile phones, smartphones, printers, removable storage devices, digital cameras and other peripheral devices, owned by the Council or 3rd Parties.

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 'INFORMATION SECURITY 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 Statements

Note: These policies apply to all in scope of section 3 of this policy.

5.1. ICT Access Policy

Users of the Council's ICT facilities will be made aware of what the Council considers to be acceptable use and their associated responsibilities of ICT access and will be granted access only on completion of an authorised joiners form (located here ICT Access request form)and a user policy acceptance form (DBC099 ISF) in order to gain access to the Council's ICT systems.

The Council's ICT systems must not be used to operate a personal business.

Each user must have a unique UserID and a password. It is a user's responsibility to protect their User ID and password and they must not divulge them to anyone.

It is a user's responsibility to prevent their UserID and password being used to gain unauthorised access to Council systems

5.1.1. Password Policy

Users will be required to change their password every 90 days and ensure that passwords contain at least three of the four following types of characters:

1. Lower case characters
2. Upper case characters
3. Numbers
4. ‘Special’ characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.).

The following password guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they areopen to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Password history is stored for up to eight instances, and minimum password length is six characters
- User access rights must be review at regular intervals
- 3rd Party suppliers must not be given the details of how to access the Councils network without the explicit consent of the ICT Service. Remote access passwords for 3rd Party suppliers must be disabled by default, and enabled ONLY via contacting the ICT Helpdesk in the first instance

5.2. Computer Usage Policy

Legislation

The principal piece of legislation is the **Computer Misuse Act 1990** which secures computer material against unauthorised access or modification. A breach of this Act is a criminal offence: a user convicted under this Act may receive an unlimited fine and a prison sentence of up to five years. The three categories of criminal offences under the Act are described below.

Unauthorised access

It is an offence to gain access without authorisation as a preparation for a further offence, whether or not that further offence is actually committed. This would, for example, include using another user’s username and password for any reason, or attempting to access another user’s files without that user’s express permission.

Unauthorised access with intent

It is an offence to use a computer to gain access to any program or information to which the user has no authorisation to access or use. This would, for example, include access to financialor administrativedata by unauthorised individuals.

Unauthorised Modification

It is an offence to make any modification to any program, file, data, electronic mail message or other computer material belonging to another user without the permission of that user. This would, for example, include the unauthorised destruction or alteration of another user's files, the creation, introduction or forward transmission of a virus, changing examination results and deliberately generating information to cause a system malfunction.

Other relevant legislation;

- Copyright Design and Patents Act 1988
- Data Protection Act 1998
- Defamation Act 1996
- Obscene Publications Act 1959 & 1964
- Protection of Children Act 1978
- Criminal Justice and Public Order Act 1994
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Pornographic Material

No one (Section 3.1) shall view or download inappropriate images (e.g. images which show violence or are pornographic, obscene, discriminatory or otherwise offensive in nature), or store such images, on any DBC laptop, PC or network drive. Viewing, downloading or storing such images will be regarded as system abuse. Individuals will be subject to The Council's conduct procedure for any such actions and may face dismissal.

Protection of Children

The Protection of Children Act 1978 (as amended) deals with photographic representation (including pseudo photographs) and data stored electronically or manually of children under the age of sixteen.

It is an offence to possess, take, make, permit to be taken, distribute (or intend to distribute), show (or intend to show), publish or have published an indecent photographic representation of such children or persons.

No individual may hold in files (or Web Pages), or transmit electronically, data which constitutes indecent material of this nature. In this context, the individual is entirely responsible for the content of his or her files, Web pages and messages.

A breach or suspected breach of this policy by anyone within scope of section 3 of this policy will be subject to procedures in section 4 of this policy.

An individual that has committed an offence under the Protection of Children Act 1978 will be subject to the appropriate action under Section 4 of this policy.

5.3. Internet Usage Policy

Access to the Internet will be permitted to authorised users by their line manager(s) unless otherwise advised.

At the discretion of your line manager, and provided it does not interfere with your work or productivity, the Councilpermits the use of the Internet facilities for non-business research or browsing during lunchtimes or before/after flexi-time/normal working hours.

Internet sites containing material relating to pornography, paedophilia, race hate, discrimination, music, gambling and gaming are prohibited.

The Council's ICT department will employ technology solutions to attempt to block such sites but it is still the responsibility of the user individual to not attempt to access sites of this nature.

All Internet access and attempted access is recorded automatically, by ICT systems.The ICT systems are updated to include blocked sites. If a user has encountered a web-site, that includes, pornography, paedophilia, race hate and gambling, then the site must be reported to ICT for inclusion in a blocked list.

All requests to remove access to blocked sites, for business purposes only must be authorised through the line manager. ICT will unblock the site providing it does not violate other conditions in this policy.

In accordance with relevant legislation the Council will review Internet access on a regular basis. A process of formal authorisation can be initiated by a manager where an individual's Internet access is suspected of violating this policy and further investigation is merited.

Except where it is strictly and necessarily required for your work, for example ICT audit activity orother investigation, you must not use your Internet accountto:

- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business.

- Download any software that does not comply with the Council's Malicious Code Policy.

The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive.

"Unsuitable" material would include data, images, audio files or video files the transmission of whichis illegal under British law,

5.4. Email Policy

All users should be aware that email usage is monitored and recorded centrally by ICT systems. The monitoring of email (outgoing and incoming) traffic will be undertaken so that the Council;

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.

All emails that are used to conduct or support official Dacorum Borough Council business must be sent using a "@dacorum.gov.uk" address. All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format "@dacorum.gcsx.gov.uk".

Non-work email accounts **must not** be used to conduct or support official Dacorum Borough Council business. Councillors and staff must ensure that any emails containing sensitive information must be sent from an official council email. Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email *(please also refer to DBC070 IS Policy - GCSX Acceptable Usage Policy)*. All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000.

ICT facilities provided by the Council for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of PROTECT or RESTRICTED material concerning the activities of the Council.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.

- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called ‘flaming’ - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the Council into disrepute.

5.4.1. Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of Dacorum Council’s anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to the Council’s outsourced IT provider.
In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access Council facilities.
- Must not forward virus warnings other than to the Council’s ICT Helpdesk or Information Security Officer.
- Must report any suspected files to the Council’s ICT Helpdesk or Information Security Officer.

In addition, the Council will ensure that email is virus checked at the network boundary and at the host, and will use the appropriate independent virus checkers.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Malicious Code Policy (Section 5.5)

5.4.2. Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party..

Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using Dacorum Borough Council systems.

If in doubt please contact the ICT Helpdesk or Information Security Manager.

A breach or suspected breach of this policy by anyone within scope of section 3 of this policy will be subject to procedures in section 4 of this policy

5.5. Malicious Code and Anti-Virus Policy

The objectives of virus protection are to ensure business continuity and minimise business damage by preventing and minimising the impact of viruses and malicious software. This policy aims to reduce the risks of damage by viruses and malicious code to an acceptable level.

The Dacorum Borough Council acts to protect the integrity of its software and its other information assets against the introduction of malicious code (malware). Specifically:

The Council formally prohibits the use, on any information processing system or device it owns or operates, of any software whose procurement was not carried out through the Council's procurement procedure or approved by ICT.

Software that has been obtained, and any other files or folders, may not be transferred or downloaded onto the Council's network via or from external networks, or on any medium (including CD-ROMs, USB sticks), including during maintenance and emergency procedures, unless specific controls have been implemented and authorised

Monitoring, detecting and deleting unauthorised software is a requirement of the information system, and disciplinary action is to be taken against anyone in breach of the Malicious Code and Anti-Virus Policy.

The Council acts to identify and patch software and system vulnerabilities in order to reduce the risk of malware attacks.

The installation and maintenance of anti-malware software or anti-virus software on all servers and workstations / laptops is mandatory

A breach or suspected breach of this policy by anyone within scope of section 3 of this policy will be subject to procedures in section 4 of this policy

5.6. Asset Management Policy

It is the intention of the Council's ICT service to control all ICT equipment and software used in an efficient manner, ensuring continuing and provable legality of licensing in compliance with the laws relating to copyright.
In order to gain, and maintain control in this manner, it is essential that control of all ICT related equipment and its associated software are centrally handled.
It is also the intention of the Council's ICT service to ensure that all ICT equipment is disposed of in accordance with best practices for data disposal as per the requirements of the WEEE directive.

There will be central responsibility for the procurement of all software and ICT related hardware used throughout the Council, the installation of the software or hardware to a user location and any subsequent movement to an alternative location. All ICT items will be ordered by, and delivered to, the ICT department only.

ICT will retain responsibility for maintaining a register of all ICT assets, both software and hardware.

A means to control all software licences will be maintained for all software used throughout the Council in order that unlicensed software may be identified. Software which is licensed, but unused, can also be identified and removed from a PC and re-allocated as required.

Where auditing shows software in use within the Council for which no licence exists, the software will be removed from the PC in question, or, if the software is required for business use, the user department will be required to pay a licence fee.

A breach or suspected breach of this policy by anyone within scope of section 3 of this policy will be subject to procedures in section 4 of this policy

5.7. Telephone / Fax and Desk Policy

5.7.1. Telephones

The Council's policy for telephones relates to the use of Council owned static and mobile telephones.

Telephones (land-lines and mobiles) - must not be used for any illegal, defamatory or obscene purpose. Personal use of telephones is acceptable, subject to the following:

- The use is legal.
- The use does not impinge on the member of staff's work or that of other officers.
- The use is not connected to any business or profit making venture.

There are a number of customer care standards which cover the various ways our customers contact the Council. Employees need to be aware of the required standards which can be found on the Council Website

Health and safety – before using mobile phones in vehicles staff and Members should refer to the latest guidance from Corporate Health & Safety.

Monitoring – the Council maintains records of telephone calls which can be identified against an individual number. Itemised call logging data will be supplied on a service unit basis to line managers periodically to be used to identify any unusual trends.

The misuse of the Council's telephone services is also considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action.

5.7.2. Fax Policy

Confidential or restricted information should not be transmitted using fax machines. If you are in any doubt regarding whether information is confidential or restricted then you should seek advice from your manager or the Council's Information Security Manager.

5.7.3. Clear Desk Policy

The Council has a clear desk policy in place in order to ensure that all restricted and confidential information is held securely at all times. Work of this type should not be left on desks unattended and should be removed from view when unsupervised.

At the end of each day it is the employee's responsibility to clear their desk of all documents that contain any Council PROTECT or RESTRICTED information, or any information relating to clients or citizens. Unclassified material, together with non-Council specific operating manuals may be left tidily on desks.

The Council PROTECT or RESTRICTED information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

Nothing should be left lying on printers, photocopiers or fax machines at the end of the day.

Users of ICT facilities are responsible for safeguarding data by ensuring that equipment is not left logged-on whenunattended, and that portable equipment in their custody is not exposed to opportunistic theft. ***(Remember to lock your computer).***

5.8. Social Media Policy

The Councils social media policy ***"Council social media usage protocol service specific 2012"*** is located on the SharePoint Intranet site here; Document Centre; Policies; Policies

A breach or suspected breach of this policy by anyone within scope of section 3 of this policy will be subject to procedures in section 4 of this policy

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 (Legal, Democratic and Regulatory) 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 and DR Manager 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. DBC900 IS - Information Security Incident Reporting Policy
7.1.3. DBC100 IM - Data Protection Act 1998 Policy
7.1.4. DBC150 IM - Freedom of Information Act 2000 Policy
7.1.5. DBC170 IS - Government Connect (GCSx) Acceptable Use Policy
7.1.6. DBC700 IS – Remote and Home Working Policy
7.1.7. DBC999 IS Proc – Information Security Incident Reporting Procedure.

8. Review of the Corporate Information Technology Security 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. Document Control

Author:	John Worts - Information Security Manager
Owner:	Steven Baker, Assistant Director – Legal, Democratic & Regulatory
Document Number	V1.1
Full Document Title	DBC010 IS Policy – Corporate Information Technology Security Policy

Revision History

Revision Date	Previous Revision Date	Previous Revision Level	Summary of Changes	Changes Marked	Next Review Date
24/5/12	n/a	n/a	Rewrite of existing Policy documents to include previously separate ICT polices to form one information technology policy document.		May 2013
13/6/12	24/5/12	0.1	Include ICT unblock of business sites, in internet policy sub-set		June 2013
27/6/12	13/612	0.2	Minor Changes following review at CMT		July 2013
11/7/12	27/612	0.3	CMT Approved FINAL		July 2013
22/8/12	11/7/12	1.0	Added 5.8 Cross reference to Councils social media protocol.		August 2013

Distribution List:

Name	Title	Date of Issue	Version
CMT		27/6/12	0.3
Mark Brookes		27/6/12	0.3
Barbara Lisgarten		27/6/12	0.3
ICT Management		27/6/12	0.3
ICT / Comms		22/8/12	1.1

Document Approvals

Version	Approved By	Date
1.0	CMT	11/7/12
1.1	ISM	22/8/12