# ICT POLICY DOCUMENTS

<table>
<thead>
<tr>
<th><strong>Author:</strong></th>
<th>ICT Operations Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Owner:</strong></td>
<td>Head of Customer First</td>
</tr>
<tr>
<td><strong>Document Revision:</strong></td>
<td>Version 1</td>
</tr>
<tr>
<td><strong>Date:</strong></td>
<td>6 September 2007</td>
</tr>
</tbody>
</table>
CORBY BOROUGH COUNCIL

ICT POLICY DOCUMENTS

1. Background

This document contains a set of policies governing the use of ICT facilities at Corby Borough Council, including PC's and laptops, PDA's, tablets and other portable devices, all software and business systems, all communications facilities and any other hardware or software capable of storing any form of data or connecting to the Corby Borough Council network.

All staff, temporary or permanent, in any role, and elected Council members, are required to indicate their acceptance of the provisions of these policies in order to have access to any of the facilities mentioned above. These documents should be treated as an extension to Financial Regulations and Standing Orders, and non-compliance with them may result in disciplinary action being taken against the offender.

It is the responsibility of each member of staff to adhere to the Policy. All managers are directly responsible for implementing the Policy within their business areas, and for their staff's adherence to it.

2. Contents

1. Security Policy
2. Acceptable Use Policy
3. Change Management Policy
4. New Systems Policy
5. Portable Device Policy
6. Remote/Mobile Working Policy

3. Compliance

The contents of these policies are designed to ensure, amongst other things compliance with the legal requirements of the following:

- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Local Government Act 1988

And other computer related legislation as required.
CORBY BOROUGH COUNCIL

ICT SECURITY POLICY

1. Background

The objective of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. Corby Borough Council is committed to the secure keeping of all the Borough’s information assets from all threats, whether internal or external, deliberate or accidental. This includes the information stored on its computers, transmitted across its networks, printed out or written down on paper, stored on film, video, tape or disk, sent by fax or spoken in conversation and over the telephone.

2. Network security

Network ID’s and an initial password will be issued to all members of staff who have signed the ICT policy documents, following a request from Human Resources, in accordance with agreed procedures. Access will be granted to business systems when requests have been received by the appropriate person (line manager, authorised data owner) using the ICT Helpdesk request forms. Where there is a local business administrator (e.g. Civica Financial Management Systems, Orchard Housing system), requests for access should be addressed to the relevant administrator.

Under no circumstances should passwords for network or business system access be disclosed to anyone except authorised members of ICT, for bona fide business purposes. Actions will be logged against individual ID’s and the use of another person’s ID and password is strictly forbidden and constitutes a disciplinary offence. If a member of staff realises that their password has been compromised, they should notify ICT immediately, and change the password.

3. PC and laptop security

If a member of staff needs to leave their desk unattended and their PC switched on, the PC screen should be locked.

Laptops should be kept in a secure location when taken offsite, and should be locked in the boot of a car when being transported. The information contained on laptops should be encrypted, and sensitive information should not be stored on a laptop. It is the responsibility of individual members of staff to ensure that all data saved on a laptop is regularly backed up on to the appropriate area on the Council network. Any loss, theft or damage to a laptop must be reported to a line manager and to ICT immediately.

4. Anti-virus measures

All computers must be protected by anti-virus software, including those used outside the office, such as laptops. Protection will be provided by software resident on the machine and on the network.

All Heads of Service must ensure that staff are made aware of the threats posed by virus infections and that they are given appropriate training in both the avoidance of viruses and the methods of dealing with infection should it occur.

Anti-virus software will be kept up to date by the ICT section.
If a virus is detected, the ICT Help Desk should be informed immediately and the suspect PC or laptop should be left in its existing state until ICT have checked it out.
CORBY BOROUGH COUNCIL

ICT ACCEPTABLE USE POLICY

1. Background

The purpose of this policy is to ensure that all staff are aware of how the ICT resources provided by Corby Borough Council should be used, both network, hardware and software resources, and of the monitoring and reporting processes used to verify this.

2. Use of the Corby Borough Council Network

Staff must log into the network with their own ID and password at all times, and all data must be stored on the network in an appropriate location, to ensure regular backup. Files to be shared by a number of staff must be stored on the Common drive, individual users’ work should be stored on the Home drive. Access to Home drives is restricted to ICT and individual users. Access to areas of the Common drive is governed by business requirements, and may only be requested by authorised members of staff (list available from HR or ICT). Staff should not attempt to access areas to which they have not been granted permissions, nor to use applications to which they have not been granted access.

3. Use of PC’s and laptops

Only PC’s and laptops purchased by Corby Borough Council’s ICT operations team may be connected to the network.

No software of any kind may be installed on any PC’s or laptops by anyone except ICT staff; if additional software is required, and it is on the approved software library list, a helpdesk request should be logged, and a business case presented for the installation, if requested. Upgrades or configuration changes must be implemented by ICT staff. No unauthorised wallpaper or screen savers should be used, no one except ICT staff shall have access to any administrative functions on a PC. All PC problems should be notified to the Helpdesk as soon as possible, no staff should attempt to fix problems themselves, and should only attempt diagnostic or other remedial work on instruction from a member of ICT support.

Any requirements to move any computer equipment must be logged as a helpdesk request; under no circumstances should staff move their own equipment. Similarly, no attempt should be made to repair any faulty equipment, remove cables etc, a helpdesk call must be logged at all times.

Due consideration must be given to Health and Safety and environmental concerns; all PC’s must be in an appropriate location in the office and placed correctly on the desk. All PC’s and monitors must be switched off when not in use, except those identified as in constant use.

4. Use of e-mail

The e-mail system is the property of the Council and all copies of messages created, sent, received or stored on the system are and remain the property of the Council. Such messages are not the private property of any individual nor shall any individual expect there to be any personal privacy with respect to any such message, whether it be designated “private” or not.
The Council maintains the right to review, audit, intercept, access, monitor, delete and disclose all messages, including attachments, created, sent, received or stored on the e-mail system for any purpose. Use of the Council's e-mail system by an employee implies that the employee recognises and consents to the rights of the Council described above. E-mail contents may be disclosed within the Council and to third parties at the Council's discretion without further permission of the employee. The Council utilises software which assists in the monitoring of the policy and scans all e-mail messages (including attachments) for abusive, offensive and pornographic images and text.

The Council maintains its e-mail system solely for business use. The use of the e-mail system for any other purpose is a violation of the Council's policy. Unauthorised activities include, but are not limited to:

- The transmission or storage of offensive material which is of a sexual or pornographic nature
- The transmission or storage of messages containing sexual implication, racial slurs, gender-specific comments, defamatory statements, or any comments denigrating a person's age, sexual orientation, religious or political beliefs, national origin or disability
- The transmission or storage of materials that infringe copyright or intellectual property rights of any third parties
- Compromising the security of information contained on the Council's computers
- Conducting or soliciting for political, personal, religious or charitable causes other than those specifically approved by senior management
- Conducting commercial ventures outside the scope of the user's employment and responsibilities.
- Engaging in improper or illegal activities

The Council's e-mail system does not have unlimited capacity and users must have due regard for housekeeping and archiving the contents of their mailboxes. They must also refrain from activities which may overstrain the computing facilities or interfere with other employees' use of the system, such as:-

- Attaching or sending large files to multiple recipients
- ‘Spamming’ – distribution of unsolicited e-mail
- ‘Letter bombing’ – re-sending the same message to one or more recipients
- Sending or forwarding chain letters
- Inappropriate use of large groups such as ‘All_CBC’ (consent should be obtained for this from a Head of Service)

Notwithstanding the Council's right to retrieve and read any e-mail messages, such messages should be treated as confidential by other employees and accessed only by intended recipient, except where proxy rights have been granted. Messages should only be disclosed to recipients authorised to have such information.

Employees should not attempt to gain access to another employee's messages without the permission of that employee, or line manager in the event of unexpected absence. Any employee discovering a violation of this policy should report it to their line manager or to the ICT Operations Manager.

Any employee who violates this policy or uses the e-mail system for any purpose deemed improper or unreasonable by the Council, will be subject to disciplinary action.
E-mails which are sent to external organisations will contain a disclosure notice which will be placed on the e-mail template. All E-mails leaving the Council will contain this message which will be attached by the Corporate system before release from the Council.

Personal data should not be attached to external E-mails unless the individual has expressly consented to the disclosure of this information in writing as required by the Data Protection Act 1998.

The Head of Customer First has the right to suspend E-mail access pending an investigation of the alleged breach of Policy. Any abuse of this policy will be investigated under the Council's Disciplinary Policy.

5. The Internet

Individual users are responsible for their actions when connected to the Internet and must ensure that they take no action which will bring the Authority into disrepute.

Personal use of the internet is permitted during periods when staff are not "signed in" under the flexi scheme. Use of the internet will be monitored, and any inappropriate use of the internet or excessive use during working hours will be dealt with under the disciplinary policy. Access to Internet sites should be for legitimate and authorised purposes; this does not include any external business activities, including the use of online auction sites. If in any doubt a member of staff should consult their line manager. An elected Member should consult the Head of Legal and Democratic Services. Access to the following categories of website will be blocked:

- Gambling and Gaming
- Pornography
- Violence and racial hatred
- File-sharing sites such as Limewire
- Personal e-mail sites such as hotmail

A helpdesk request should be submitted by a line manager for access to any blocked site for legitimate business reasons.

CBC will not take responsibility for any financial loss or disclosure of personal or financial details as a result of staff utilising the internet using CBC network/equipment. Staff enter such details/use the internet at their own risk.

ICT will produce monthly reports of internet activity which will be circulated to line managers.

Users must take reasonable steps to abide by:-

- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Defamation Act 1996

In particular, users must consider carefully and check the use of any information about any individuals in terms of authorisation, consent, accuracy, whether it is up to date and how long it should be kept.

Users must follow all good practice laid down to avoid computer viruses.
Users must not send, display or download any material, in particular pornography, which could bring the Authority into disrepute, or anything which could be construed as defamatory or libellous. No personal information should be stored on any devices or network drives owned by Corby Borough Council.

Users must not import or copy software from the Internet or export or copy software to the Internet.

In exceptional circumstances, the Head of Customer First may grant permission to selected users for specific periods of time to evaluate the security of the Corporate facilities by probing, hacking or other means.

ICT Services may use Internet facilities to obtain updates and fixes from software suppliers, provided that any code so obtained is subject to virus checking. They may also import and must virus-check shareware or freeware for evaluation purposes, with the approval of their line manager. ICT staff may also need to use personal e-mail accounts for testing purposes only.

6. **Other ICT equipment**

All ICT equipment must be purchased through ICT, and should be requested via the ICT Helpdesk form; equipment purchased in any other way will not be installed or supported by ICT and may not be connected to the network. This includes printers, cameras, memory sticks etc. The use of such devices is covered in the Portable Device Policy.

As with PC’s, only ICT staff should move, repair or disconnect any ICT equipment.

**Printers**

Wherever possible all documents should be printed double-sided and in black and white unless there are good reasons to do otherwise. Printers and other devices should all be switched off when not in use.
CORBY BOROUGH COUNCIL

ICT PORTABLE DEVICE POLICY

1. Background

This policy covers the use of all portable devices capable of storing data; this includes (but not exclusively) portable hard drives, USB memory keys, mp3 players, cameras, mobile phones, PDA’s and all other similar devices. The use of such devices has been increasing, as has their capacity, and staff using any portable devices should observe the following:

• Only devices purchased by Corby Borough Council, recorded on the asset register and provided by ICT for work requirements may be connected to any PC owned by the Council. ICT will be implementing software which controls access to the PC so that unknown devices cannot be connected and unauthorised persons cannot connect any such devices.

• All devices will be issued by ICT to named individuals within service areas; the security of the devices and the data stored on them is the responsibility of that person, and the person using the device. No sensitive data should be stored on these devices; this includes (but not exclusively) confidential information, items covered by the data protection act, etc. If in doubt, staff should consult their line manager.

• No personal files should be stored on any such devices by any member of staff as they are for work only.

• Files should not be copied from these devices on to an individual’s own PC or any other PC or laptop not owned by the Council.

• No configuration changes should be made to any devices supplied for work purposes.
CORBY BOROUGH COUNCIL

ICT REMOTE WORKING POLICY

Background

• This policy covers the ICT aspects of staff working from remote sites or any other location which is not part of Corby Borough Council’s Wide Area Network, or where the network or internet connectivity has not been provided by Corby Borough Council. It does not cover other aspects of remote working, such as Health and Safety, HR or management issues.

• Staff may work from remote sites or from home with the approval of their line manager, and the agreement of HR and the Health and Safety Officer. Working from any remote location requires a broadband connection, as it is not practical to work from home on a dial-up connection. Only Corby Borough Council PC’s and laptops may be connected to the Council’s network, and this should be arranged with ICT. ICT will endeavour to create a connection to a user’s Internet Service Provider, if all the necessary information can be supplied, but cannot guarantee to do so, nor can they provide support for problems with a user’s Internet Service Provider.

• The Council’s e-mail system can be readily accessed using a web-based mail service, but a Virtual Private Network connection is required in order to access any data or applications on the network. This is a secure connection between the network and an individual PC, and uses a shared security key, set up by ICT. When connected through the Virtual Private Network (VPN), the PC will not be able to access any other websites directly, only through the Corby Borough Council connection. This is to prevent the creation of a ‘split connection’, creating a direct link between the internet and the network via the laptop.

• Any laptops or PC’s connecting in this way will have the latest security updates and anti-virus updates delivered to the desktop as soon as they connect. This may involve a certain delay, but this is an important security measure.

• Only authorised Corby Borough Council staff should use any Council-owned PC or laptop and staff are expected to take reasonable precautions to safeguard the equipment, the access to the network and any data stored on the PC or laptop. Laptops should be kept in a secure location when taken offsite, and should be locked in the boot of a car when being transported. The information contained on laptops should be encrypted, and sensitive information should not be stored on a laptop. It is the responsibility of individual members of staff to ensure that all data saved on a laptop is regularly backed up on to the appropriate area on the Council network. Any loss theft or damage to a laptop must be reported to a line manager and to ICT immediately.
1. I have read and understood the Policy Documents set out above and agree to abide by the Policies and Procedures as specified.

2. I understand that Internet access and E-mails will be intercepted, monitored and read in order to ensure that the content is in accordance with Council business.

Signed: ____________________________ Date: ____________________________
(Print Name) ____________________________ Department: ____________________________

Countersigned: ____________________________ (Manager) Date: ____________________________
(Print Name) ____________________________ Department: ____________________________

When the details on this page are completed, please forward this sheet to the ICT Operations Team.

You must keep the Policy Document for reference.

You will be given external e-mail and Internet access when the necessary forms have been received by ICT and HR.