Breckland Council

Information Security Policy & Guidelines

Version: 2a
July 2010

Contents

1. Introduction

1.1 General

The Council depends on its ICT systems for normal day-to-day business activities and for the development and introduction of new systems and services. Consequently any loss of the ability to access data could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide services to its citizens. It is therefore essential that the availability, integrity and confidentiality of its ICT systems and data are maintained at a level, which is appropriate to the Council's needs. All staff and Members have a duty and responsibility both to the Council and the people of Breckland to protect this asset from unauthorised use, disclosure, access, modification and destruction. This document describes the Council's IT Security Policy which is designed to achieve this.

You are required to acknowledge your agreement to comply with this IT Security Policy it by signing and returning the tear off slip at Appendix 3. Note: These signed sheets are stored with individual's staff records within HR.

1.2 Governance framework

The governance arrangements relating to this policy follow a 7-step approach that is being developed jointly by Breckland and Steria in relation to a number of elements of IT service delivery such as procurement, asset management, security, help-desk operations, etc.

Step No.	By	Activity
1	Breckland	defines its policies and standards in each area
2	Breckland and Steria	agree and document the processes to be followed and (where appropriate) their quality
3	Steria	implements the necessary processes to deliver the services to that quality
4	Steria	monitors adherence to the processes
5	Steria	Reports breaches and general performance to Breckland
6	Breckland	enforces policies and procedures through the designated governance groups e.g. CMT
7	Breckland and Steria	review these arrangements annually (Note: this to include review by Unison and Joint Consultative Committee where appropriate)

2. Scope

2.1 Who it applies to

The Breckland Information Security Policy applies to:

- all staff
- all elected Members of the Council
- all employees and agents of other organisations who directly or indirectly support or use the Council's computer systems or networks e.g. Steria/Capita Symonds.
- All temporary and agency staff directly or indirectly employed by the Council.

2.2 Where it applies

The policy remains in force regardless of location and specifically includes those who work at and Council office, at home (including Members), in the field, or any other location where the user is using the Council's IT services.

2.3 What it applies to

- All Council Information
- All physical data and voice communications networks and components
- All software applications resident on applications servers, file servers and networking equipment
- All PC systems and accompanying software applications
- All storage media including paper
- Internet and e-mail services
- Use of social media applications (Social Media Policy V1 issued july 2010 refers) – acceptance of this policy also assumes acknowledgement and acceptance of Social Media Policy also.

3. Roles and responsibilities

3.1.1 All Staff and Members -

- are required to read, fully understand, and comply with their obligations with respect to this ICT Security Policy.
- are required to report any suspected or actual breaches of this policy to the ICT Manager

3.1.2 Service Managers: -

- are responsible for enforcing all ICT security procedures and ensuring that all aspects of this computer security policy are adhered to within their service area.
- will take appropriate steps to ensure that their staff comply with the relevant legislation (see Section 5 for details)
- are responsible for identifying any sensitive information that is used within their service and for ensuring that robust security arrangements are in place for securing it (e.g. health or financial records, information about vulnerable people)

3.1.3 The ICT Manager is responsible for: -

- producing this policy and continually reviewing its provisions
- obtaining approval from CMT, Members, etc.
- communicating its contents to users and providing appropriate guidance and training
- monitoring (in association with Steria) compliance with the policy
- enforcing the policy and coordinating the Council's response to any breaches.

3.1.4 Steria: -

- is responsible for the integrity of the Council's IT services
- will implement the technical and procedural provisions of this IT Security Policy
- will maintain written procedures and ensure that their staff are appropriately trained and equipped to implement them
- will monitor IT systems through a combination of automatic and manual checks to ensure compliance with this policy
- will log and investigate actual or suspected breaches of this policy and report the findings to the ICT Manager for action

3.1.5 CMT

- Is responsible for approving this policy and ensuring it is enforced

3.1.6 HR

- Are responsible for obtaining signoff of this policy by all staff and Members and ensuring the policy aligns with the Council's employment and disciplinary arrangements

3.1.7 Audit

- Are responsible for auditing and making recommendations for improving the Council's security arrangements

4. Compliance with Legislation and other standards

4.1 Legislation

This policy is designed to ensure that the Council complies with key legislation in this area including the following:

Data Protection Act 1998	This Act was created to ensure that all personal data (i.e. data relating to a living identifiable individual) stored or processed by computers or held in structured manual records is accurate, relevant and obtained fairly, is only used for specific purposes, and is protected against misuse.
Computer Misuse Act 1990	This makes it an offence for a person to knowingly attempt to access data or systems without proper authorisation
The Defamation Act 1998	The author of a libellous message is responsible for it and liable for any damage it causes to the reputation of another. The author's employer may also be liable.
Freedom of Information Act 2000	Ensures public access to organisational records and information in the public/government domain
Human Rights Act 1998	Everyone has the right to respect for his private and family life, his home and his correspondence and… there shall be no interference by a public authority with the exercise of the right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others
The Regulation of Investigatory Powers Act 2000 (RIPA)	Monitoring (but not recording) communications is authorised for the purpose of determining whether they are personal or business communications The interceptor must make all reasonable efforts to inform every person who may use the telecommunication system in question that communications…. may be intercepted

4.2 Standards and best practice

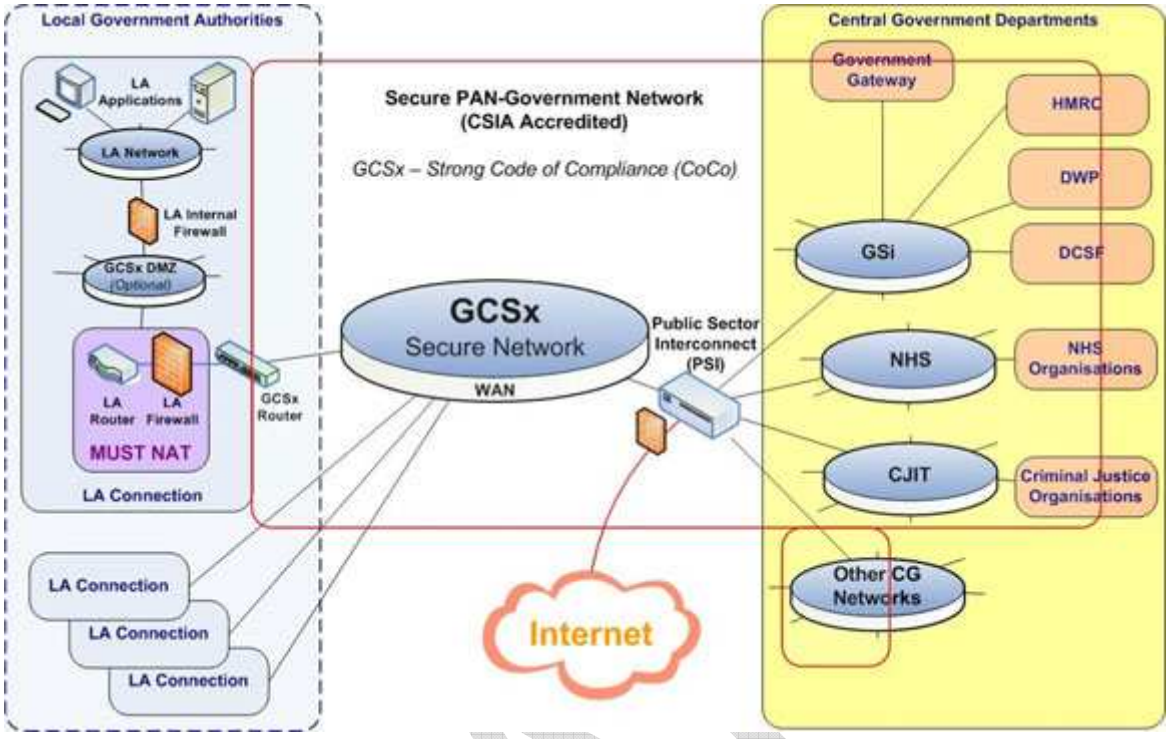
ISO27001 is a code of practice, supported by industry and the DTI. The objective of this Policy is ensure compliance with (but not certification in) those aspects of ISO27001 which are appropriate for the Council. NB There is also a drive to adopt ISO31000 Risk Management standards.

4.3 Connectivity – Government Connect obligations

The GCSX Code of Connection (CoCo) is a list of security controls with which ALL local authorities must be compliant before their GCSX circuit can be activated (this GCSX connects Local authorities with other public sector partners as shown in the diagram.)

Note: The GSi community is revising the Code of Connection that controls access to the GCSX circuits provided by Government Connect. All local authorities will be assessed against Code of Connection 4.1. Brecklands assessment is due in Jan 2011:

Diagram of GCSX connectivity model



5. Monitoring and enforcement

5.1.1 General

The Council's Communication Systems are designed to help employees in the performance of their work. Negligent improper or unlawful use of the Council's Communication Systems may create legal obligations for or lead to criminal prosecution against any Employee or the Council. The Council will not tolerate abuse, unauthorised or unsecured use of its Communication Systems.

Breach of any term of this Policy may lead to disciplinary action or to termination of any engagement supplier of any IT goods/service. It may also result in civil or criminal action being taken against any employee and / or the Council. An example of a breach may result from the use of the Council's computer to access websites with unsuitable contents such as child pornography, etc. See below for examples of major and minor Breaches.

The Council reserves the right to monitor Internet & Email usage by staff and Members. Random checks on PC's, Laptops & PDA's will also be carried out to ensure that unlicensed or trial software is not installed on the Council's ICT equipment.

5.1.2 Examples of breaches

Breach	Category
Copying or sharing with others software, music or movies without the written permission of the copyright owner.	Major
Hacking into, meddling with, or damaging any other computer or service. e.g. trying to "break into" or "crash" another computer on the Internet.	Major
Possessing, accessing or using any unauthorised hacker tools, whether hardware or software based. e.g. "packet sniffers" and "password crackers".	Major
Viewing, downloading, storing, sending, or giving access to material deemed as objectionable by the Censorship Act 1996 (WA). eg. materials such as child pornography, incitement to violence, torture, and bestiality.	Major
Harassing any person e.g. sending obscene messages, language, pictures or other materials; issuing threats of bodily harm; contacting a person repeatedly without legitimate reason; disrupting another person's lawful pursuits; and invading another person's privacy.	Major
Unauthorised use of access accounts and/or passwords: • Deliberately • Inadvertently	 Major Minor

Please note that breaches are not necessarily limited to those outlined above.

5.1.3 Dealing with breaches

Breaches of security must be reported to either the ICT Manager or the Steria Service Manager as

soon as possible. Steria will record any breaches by means of a formal logging and follow-up system (note that this may require Steria to upgrade their existing systems). For each incident, this will include the investigation of the problem cause, options for the prevention of recurrence, maintenance of an audit trail, informing those affected; ensuring recovery is achieved with minimal delay and the management of a review process. The audit trail will be suitable for internal statistical analysis, and for use as evidence on contractual and legal issues such as computer misuse and data protection.

The responsibility for the recovery from an incident or failure will be restricted to staff with specific support responsibilities.

Where a breach is discovered the ICT Manager will undertake the appropriate enforcement action. For minor or inadvertent breaches this may include:

- Technical changes to physically prevent further such breaches
- Informal warnings regarding future behaviour
- Informal warning to the Service Manager

For major or persistent breaches by staff the Council's disciplinary procedure will be invoked and could result in dismissal.

For major or persistent breaches by Members the Council's Constitution and Members' Code of Conduct will apply.

6. Security policies

6.1 General

All computer systems are for the sole use of the Council. The Council owns all data that exists on these systems and has the right to access, edit and delete it.

All of the Council's server, WAN and associated LAN data and voice communications equipment are managed by Steria. Data networks are managed in such a way as to prevent unauthorised logical and physical connection, and to detect unauthorised connection should this occur. Data communications protocol filtering mechanisms are also employed to restrict network access to authorised users.

No unlicensed or unauthorised software is permitted on any of the Council's ICT systems. Trial or evaluation software should not be installed on the Council PCs or laptops without the consent of Steria and ICT Manager.

Downloadable files must not be installed on Council equipment except by Steria or by their direction.

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is prohibited.

Steria operate formal change control procedures prior to implementing any request to install/upgrade/change any application software. For this reason you must contact the Steria helpdesk on ext.499 or 01842 756499 well in advance otherwise the request may be rejected or work delayed.

It is unlawful to reproduce copyright material without the express permission of the copyright holder. Staff and Members must not use the Council's Communication Systems to access, transmit, retrieve, download, upload, store, distribute or otherwise process any material the copyright for which is or they suspect may be owned by a third party (without the prior authorisation of the copyright holder).

It is the responsibility of Service Managers to identify any data that is of a particularly sensitive nature (and where it is stored). They must also determine whether any specific security precautions are to be taken over and above what is specified in this document and notify these in writing to the ICT Manager.

6.2 Procurement

Before any ICT hardware or software is procured, or commitment is made to procure, formal approval will be required from the appropriate capital or revenue budget holder. In most cases this will be the ICT Manager and if not, it will require his/her express and prior approval.

All purchases of software must be carried out by the ICT Client Unit. You are forbidden to purchase software/hardware from third-party suppliers without prior written agreement from the ICT client unit .

There are forms available on the Biz for requesting new/upgraded PCs and laptops for incoming staff.

6.3 Inventory

Steria maintain a computer-based ICT Inventory Register. This Register includes all major items of ICT

hardware, such as applications and file servers, PC equipment and telephony equipment, but will exclude minor equipment such as telephone handsets and connection cables. A separate register will include all software applications owned or licensed by the Council.

6.4 Physical security

Only authorised persons are allowed access to the secure computer rooms. Emergency access for Health and Safety purposes can be gained by contacting the Steria Help Desk [x499] or the ICT Manager (or ICT Deputy in absence of ICT Manager).

The disclosure of door access codes, or supply of security swipe cards, to unauthorised personnel is not allowed [except when prior written permission from your Service Manager is obtained]

Keys for secured areas, equipment cabinets and cupboards must not be handed to unauthorised staff.

Any access to any secure area is recorded on a separate sigh off sheet.

6.5 Use of Computer equipment

6.5.1 Safe custody

Service Managers are responsible for the safe custody and use of the computer equipment within their service areas and should be aware of the location of all portable equipment within their service at all times and in the event of an audit.. Such responsibility may be discharged through delegated officers and, for Steria staff, through the ICT Manager.

Laptops are unfortunately easily stolen. When not in use they should be stored in a locked cupboard. This also applies to portable printers together with any other portable equipment such as Laptops, PDAs, Blackberrys and Mobile Phones. Such equipment must not be taken off site without prior approval of the service manager.

IT equipment must not be left unattended and in full view in a vehicle, as it is not covered by the Councils insurance. If equipment is left unattended in a car for any reason, you should store this equipment in the trunk of their cars for safekeeping.

6.5.2 Use of PCs

You must not in any way change the existing configuration of the Council's software, desktop or Laptop. [suitable personalised static images are acceptable as a screen backdrops.]

Trial or evaluation software must not be installed on Council PCs or laptops without the consent of Steria/the ICT team who will undertake the loading of all software onto PCs including any non-standard software such as shareware or screen savers which can sometimes be detrimental to the performance of the PC.

Files (documents, spreadsheets etc) saved locally to the PC on the C drive are not backed up by Steria. If the C drive is damaged or otherwise unusable the data on it cannot be recovered. For this reason Council data should not be held on the C drive.

Citrix users are secured by the file server backup processes, and risk of data loss is minimised, as all network drives are backed up by Steria.

PCs should not be left unattended whilst logged onto the Network. However an auto log off function is in operation to prevent someone else using your PC while you are away from your desk.

6.5.3 Use of printers

There are no security arrangements with regard to using printers. General guidance on how to use printers effectively, the use of duplex, and other measures to minimise paper usage are available within the Print Strategy document – issued 2010.

6.6 Virus protection

Proactive measures are taken to safeguard the integrity of software and data by detecting and counteracting the effects of 'malicious' software such as computer viruses. Anti-Virus software is installed on all servers, PCs and laptops and kept up to date by Steria. Virus detection software is also deployed on 'gateway' equipment (such as firewalls, mail and proxy servers) as appropriate.

All incoming files, programmes and e-mail attachments via email and the internet are automatically scanned before they are allowed into the network. If you detect a virus on any file programme or e-mail attachment you must report this immediately to the Steria Help Desk on ext499.You should not forward chain email letters or email virus warnings from other sources as this is a common way of distributing the viruses themselves: all virus warnings will come from Steria.

6.7 Access Control

6.7.1 User "permissions"

Access to the network and the IT services available on it is controlled by Steria: users are given network "permissions" according to their job requirements. A Service Manager can request extensions to such permissions (e.g. which network folders the user is allowed to access, or which features of Microsoft Outlook are available to him/her)

Each major software application will have a similar policy regarding user access permissions which is defined by the system "owner" in association with Steria This policy will define:

6.7.2 Allocation of userdIDs and passwords

Network passwords are allocated by Steria (NB Application passwords are issued by business system owners)

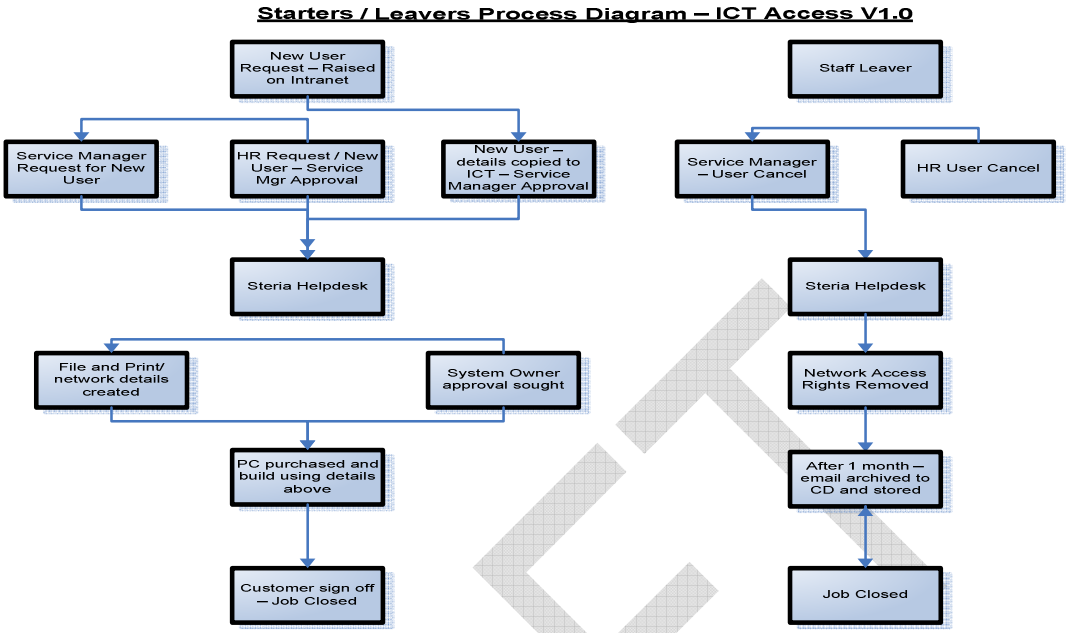
The initial allocation of passwords, and any resetting of forgotten passwords, will be formally authorised by the service owner of the software application by application to the Steria Helpdesk.

Service owners are responsible for reviewing users of their systems at regular intervals and for removing users who have left.

The Council's HR section will be responsible for notifying Steria, on a monthly basis, of starters and leavers or where staff change job function so that their access rights can be modified.

Add/Change/Delete user process:

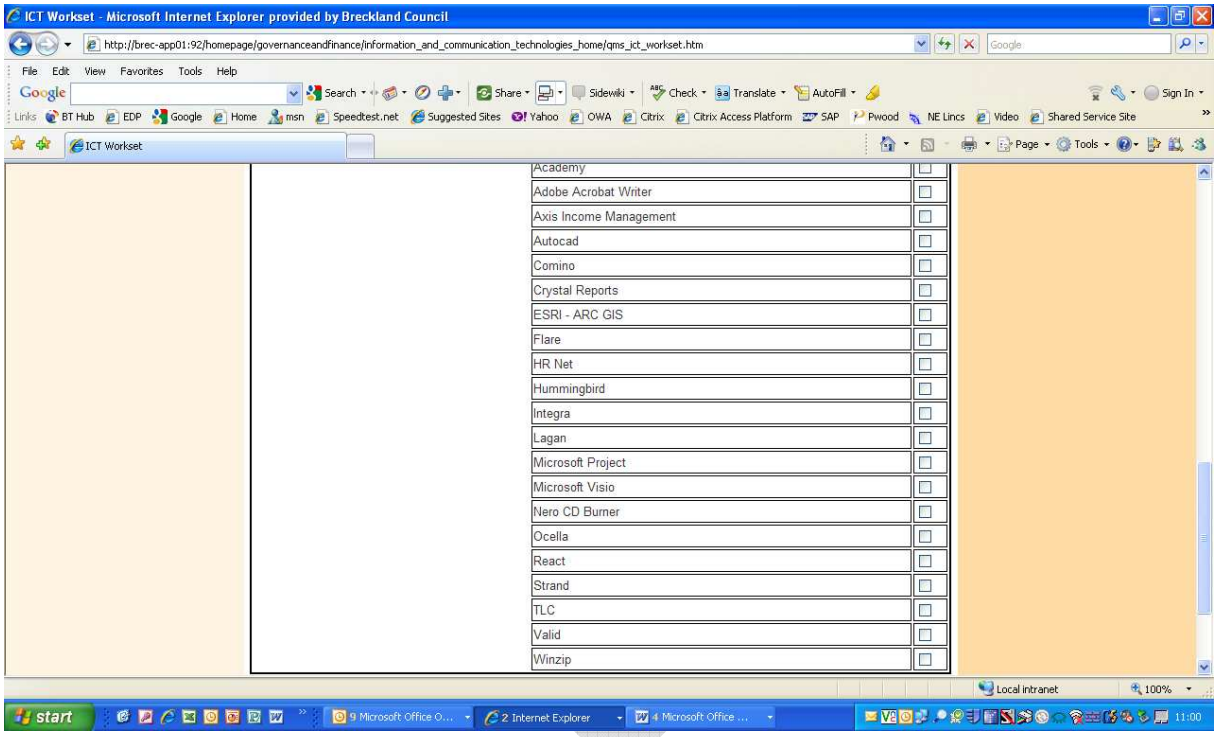
The diagram below shows an overview of the process to add/change/delete users from the network



New Starters/Changes/Leavers process is initiated by either Service Manager or HR raising a request via the Intranet (see http://brec-app01:92/homepage/governanceandfinance/information_and_communication_technologies_home/ict_requirements_forms.htm) or via separate email to Steria Helpdesk. When new user/leaver details are confirmed, hardware is ordered (if new user) and a standard build PC/laptop is built, with access to key systems being granted via system owners. When finalised, PC/laptop is installed and new user details are tested with key applications. New user password also set to force change at first login – default being 7 digits, needing both an alpha and a numeric and upper/lower case characters to comply with our Govt Connect obbligations.

The process is initiated via the ICT pages on the Breckland Intranet (see link as follows) http://brec-app01:92/homepage/governanceandfinance/information_and_communication_technologies_home/ict_requirements_forms.htm

Steria create 'basic' user access, including inter and intranet access, with key system access granted by key system owners, further info as follows:



Authorisation is required at Service Manager/Line Manager level for standard access and system owner level for specific access – with new users being provided a 'once only' password forcing a change at first login.

System Owners and Service Manager/Line managers will be required to periodically review continued access needs, based on business requirements.

6.7.3 Use of passwords

Passwords must not be disclosed to or shared with anyone else.

Passwords must not be written down.

Passwords should be a minimum of six characters, both alpha and numeric, and should be changed at least every two months - to a previously unused password that is not in the same theme as the last one. NB Password policies may change according to application.

6.8 Internet usage

You must only access the Internet through the Council's Internet Provider by use of software and hardware installed for that purpose by Steria. Users will not be permitted to change in any way the configuration of the software used e.g. Internet Explorer.

You are permitted to access the Internet for personal use on a limited basis and in your own time (usually during the lunch-break) but only with the approval of your Service Manager and as long as this does not interfere with your job responsibilities.

Internet usage is monitored by Steria and the IT Manager: unauthorised use is a major breach of this policy. NB Internet usage stats are recorded and issued on Monthly

You are expressly forbidden from downloading any software or other executable programs. If you identify a need to download software from the Internet for evaluation purposes, you must first contact your Service Manager to make special arrangements. Software must not be downloaded in advance of these discussions since the act of downloading may make the Council liable to purchase the software on the supplier's terms and conditions of contract.

You should neither download nor transmit any material that is pornographic, racist, sexist, of an extreme political nature, or which incites violence, hatred or any illegal activity or otherwise may bring the Council into disrepute nor information, which could be regarded as sensitive.

6.8.1 Using email

All external e-mails and files exchanged over the Internet will pass through one of the Council's 'Firewalls' to prevent the spread of viruses and malicious software. However, this is not a complete answer to the problem and any suspicious e-mail or attachments should not be opened. You must report any suspicious e-mails or attachments to their manager and the inform Steria immediately on x499.

E-mail is not totally secure and no personal, confidential or sensitive material should be sent by e-mail or attached to any e-mail, without careful editing and consideration.

All e-mails to external sources will include a disclaimer.

There is an etiquette associated with composing and sending emails, with the main features are:

- Never assume that a message you have sent has been read.
- Make arrangements for your e-mail to be forwarded to, or accessed by, someone in your absence. Consider the use of an automated reply system to warn the sender.
- Never send abusive or defamatory messages.
- Use an e-mail 'signature' in accordance with the Council standard
- Never send or forward chain letters or other 'unsolicited' mail (SPAM) such as 'virus or other warnings' or advertising. Resist the temptation to copy any message to more people than is necessary.
- Never send any message that might discredit or embarrass the Council.

Note: If you are required to send email containing personal information to DWP, you will need to apply for a Govt Connect email account in format of <name>.Breckland.gsx.gov.uk – this request needs to be made via the ICT Team.

6.9 Working at home or at a remote location

Some staff and all Members use the Council's IT services at home or at another remote location: all aspects of this policy still apply to them. Before working from home you should request a health-and-safety risk assessment to ensure that your working environment (e.g. power supply) is safe and fit-for-purpose, and that Data protection obligations can be met through external working.

The Council provides a number of different methods of remote connection to IT services and restricts

those parts of the network and software applications that are available to occasional home/remote workers. The Council now employs Citrix as its remote connection tool, ensuring that data remains securely within the Breckland infrastructure – this is also a key requirement to meet its Govt Connect obligations.

The process to request remote access is as per following

Remote User Request Process Diagram

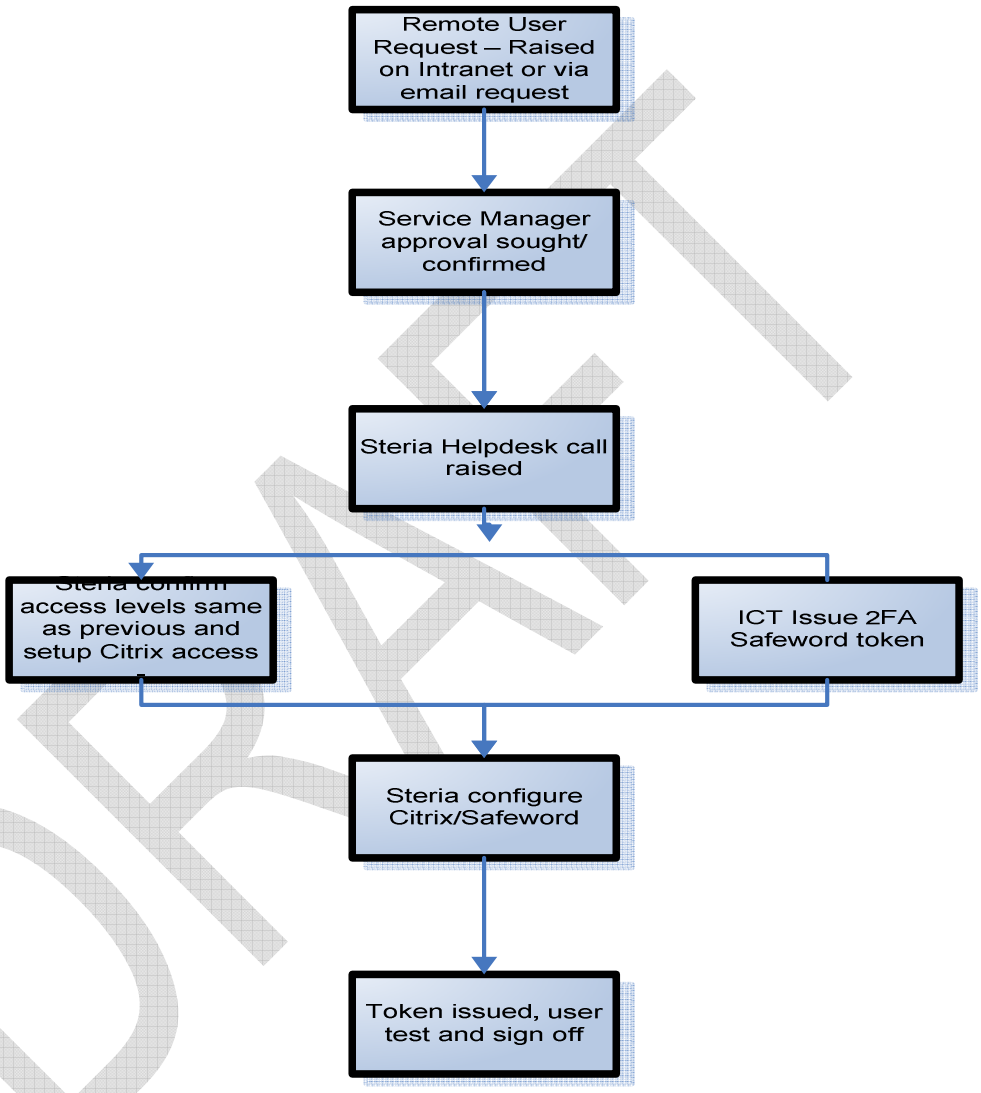


diagram:

As part of the Council's obligations regarding Government Connect – all remote users must have local drive encryption installed – and use the Council's 'Safeword' 2 factor token to authenticate on the network.

External access to the Council's ICT infrastructure and systems (e.g. by suppliers) is not permitted without prior authorisation from the Council's ICT Manager. Note all 3rd party suppliers will also be required to adhere to Code of Connection policies, and use two factor authentication (2FA) to connect to council services.

6.10 Mobile phones/Blackberry's/Portable Devices

Please see the Council's Mobile Device Acceptance Form (issue 2010) to request a mobile device.

Council provided mobile devices are the property of Breckland Council and should be used for legitimate business purposes only. Communications devices capable of transmitting and receiving data information, such as Personal Digital Assistants, certain mobile phones, Blackberry's, and laptops should only be used for the purposes for which they were supplied.

Users **must not** use, try to use, or let anyone else use staff mobile communications devices for:

- Anything that is illegal or immoral;
- Making offensive, threatening or harassing calls;
- Use of the Short Message System (SMS), multi-media messaging or email to send or receive inappropriate or offensive remarks, graphics or images;
- Use in contravention of Regulation 104 of the Road Vehicles (Construction & Use) Regulations, 1986; i.e. using a mobile device whilst driving.

The sending or receiving of SMS text messages for the purposes of downloading, or otherwise accessing, ring tones, games, commercial competitions, sports report services and other non-business related activities or applications is **not permitted**.

Users have a responsibility to utilise the Breckland Council's communications resources and services in a manner that is consistent with the Breckland Council's standards of business conduct.

Mobile communications devices should be securely stored when not in use. Handset covers provide a degree of physical protection and can be provided with mobile handsets. Users may be liable for repair or replacement costs, should their handset be damaged or lost. Any such damage should be reported to the Service Manager, and to the ICT Department, you may also be required to contact the Police for an incident number in the event of loss or theft.

6.11 Backups

The ICT Manager in conjunction with Steria are responsible for ensuring that all applications, data and operating environments on the network are adequately backed up and copies of those backups are stored in a secure, off site location. Steria operate back-up and recovery procedures designed to permit recovery as rapidly as possible.

As described earlier, data held on the C drive of a PC or laptop is not backed up at all.

Following the departure/resignation of an employee, Steria will deactivate the account following confirmation of change from HR and ensure that emails and files related to the employees job function be stored or archived for a period of at least 6months before being deleted. This is important to ensure that an audit trail is maintained of any important issue regarding the work the employee was responsible for prior leaving the Council.

Steria will be responsible for archiving data held on file and applications servers and other corporate ICT equipment.., from all major and minor problems, including media failure, human 'error', theft of equipment or a major disaster such as fire. For all critical and corporate file and applications servers, sufficient back-ups will be held at remote sites to enable the recovery of all systems should a disaster

at any one Council site result in the complete permanent loss of ICT facilities at that site.

6.12 Business continuity and IT disaster recovery

Steria provide a limited Disaster Recovery service for key Council servers/applications such as Council Tax, email, etc. Steria also maintain a documented DR plan for the recovery procedures which is regularly tested.

If invoked, the DR service will provide for new key servers to be delivered to a location of the Council's choosing within 48 hours. The location will be Hounslow, by default, and there is the option to bring a limited service to either Elizabeth House or Breckland House. At this point Steria will recover these key servers/applications from backup tapes one-by-one. This process along with connecting displaced users to the recovered systems in accordance with the Business Continuity Plan. Please note: Data connection speeds will be much slower than the in-house service – but does provide some limited systems access.

Note also that this is not a full business continuity service: it is simply a service which provides for the rapid recovery of core IT systems on replacement servers at a location of the Council's choice following a disaster. It does not cover accommodation, documentation, furniture, recovery of non-IT services, providing displaced users with PCs, etc. All of these are covered in the Business Continuity Plan for the Council as a whole supported by Service/Team plans.

6.13 Exchanging data with external organisations

The physical or electronic exchange of any software and/or data between the Council and external bodies should be subject to formal agreement which include the identification of data formats, carrier arrangements and documented verification of receipt.

Appropriate standards will be applied to the electronic exchange of data between the Council and external agencies. Wherever practicable, software applications that depend upon Electronic Data Interchange (EDI) facilities should include precautions to deal with the possibility that data has been intercepted or modified during transmission, along with checks that data has been dispatched and delivered correctly. Data that has been identified as being of a specifically sensitive nature will not be transmitted unencrypted across unsecured EDI links. Such data may be transmitted unencrypted across secure EDI links or other secure networks such as the Government Secure Intranet. All security controls applied to EDI links will be agreed with the relevant trading partners and compatibility with industry standards will be sought wherever possible.

You must not communicate any "personal data" (as defined under the Data Protection Act 1998) about staff or Members without the prior authorisation of the Human Resources Manager.

3rd parties that need to connect to us are also required to adhere to Code of Connection policies.

Freedom of Information and Data Protection

The Council has published guidelines on arrangements for compliance with Freedom of Information and Data Protection legislation. For details click the links below:

http://brec-app01/theBiz/records_management_policy_-_sep_2004.doc

http://brec-app01/theBiz/data_protection_policy_-_sep2004.doc

6.14 Disposal of information and IT equipment

All waste paper must be disposed off with due regard to its sensitivity. Confidential output must be stored in the blue wheelie bins provided for this purpose. Less sensitive waste paper can be disposed off in the recycling bins.

Magnetic media, such as floppy discs, CDs, toner cartridges, etc must be disposed of by informing the ICT Help Desk, who will arrange for a suitable means of disposal.

The new Government Connect Code of Connection v 4.1 will however impose additional Data Classification markers on all data communicated by the council, this will therefore impact further on the disposal of information model Dec 2010 onwards.

6.14.1 Disposal of PCs and other IT equipment

The Waste Electrical and Electronic Equipment (WEEE) Directive came into force in January 2007 and aims to both reduce the amount of WEEE being produced and encourage everyone to reuse, recycle and recover it. For more details follow this link:

http://www.environment-agency.gov.uk/business/1745440/444663/1106248/

The following procedure should be followed throughout the disposal cycle of all end-of-life PC s and laptops.

All redundant ICT equipment will be disposed of by arrangement with ICT Services. Before disposal, the equipment concerned must be written off in accordance with Financial Regulations and removed from the Council's general asset register and also from Steria's inventory of IT equipment. All Asset, Equipment and Software licensing labels should be removed.

In the case of attached disks or other storage devices, specific care will be taken to ensure that all systems software and data are erased from disk prior to disposal of the assets. Any third party retained by the Council for disposal of equipment will be contractually required to ensure that data on faulty disks is destroyed.

Under no circumstances should redundant PC equipment be disposed off by depositing items in the Council's bins or skips.

Elements of PC systems, printers and individual components may be disposed of as General Non-Hazardous Waste.

The Council may elect to sell/donate end-of-life to charitable organisations in which case a simple specification sheet should be complete. On hand over, the recipient should sign two copies of the Transfer Sheet .The Council should retain one copy and the external body takes the second copy. An Electrical Safety Advisory Note should also be handed over to the receiving party. (See Appendix 1 for examples).

7. Special arrangements for Members

As well as being bound by all of the conditions of this policy, Members are also subject to the following additional conditions:

- Where a Member is found to be in breach of this policy any subsequent enforcement actions will be in accordance with Constitution and the Code of Conduct for Members.

- Members are provided with IT services by the Council to assist them with the fulfilment of their duties as an elected member. Use of Council-provided IT services for commercial activities is not permitted. Reasonable use of the services for personal activities is permitted.

- Members' homes should be subject to a health-and-safety risk assessment before Council-provided IT services are installed there.

8. Appendix 1 – Disposal & Recycling of Redundant PC's

REDUNDANT PC EQUIPMENT

EQUIPMENT TRANSFER SHEET

INFORMATION & COMMUNICATIONS TECHNOLOGY SERVICE

Number of PC Systems being transferred ……

Serial Numbers of equipment being transferred

System Units	Monitors	System Units	Monitors

Received on behalf of: ……
……..
……
……

By (print name) ……

(Signature) ……

Date ……

ICT Manager ……

By (print name) ……

(Signature) ……

SURPLUS PC EQUIPMENT

ELECTRICAL SAFETY ADVISORY NOTICE

INFORMATION & COMMUNICATIONS TECHNOLOGY SERVICE

The systems that you have received have been electrically tested and found safe whilst in use within the Council. The systems have been recently tested before packing for recycling.

However, as the equipment is not contained in its original packaging, and it is likely to be subject to additional handling and transportation, it is advisable for you to satisfy yourself of its electrical safety by arranging for it to be further tested when it is installed in your premises.

9. Appendix 2 - Glossary

Application	A set of specialised programs and associated documentation to carry out a particular application such as Council Tax or Planning
Backup	To save data, applications and systems. It usually consists of writing everything contained on a system or PC to another form of electronic media, such as a¼ inch tape cartridge or another hard disc. This is then available if any information is lost or corrupted.
Computer System	Is a central processor together with its associated peripheral equipment.
Data	Information or data that is stored on a computer. It can be anything from a word-processing document to a number.
E-Mail	**E**lectronic **Mail**ing System for both internal and external systems.
ECHR	European Convention on Human Rights
Hardware	The physical components of a computer system, including peripherals (e.g. processor, keyboards, screens, printers).
ICT	**I**nformation and **C**ommunication **T**echnology.
IS/IT	**I**nformation **S**ystems/**I**nformation **T**echnology.
Laptop	Portable Personal Computer.
Login name	This is the name you type when prompted. To log in to a certain system e.g. Council Tax, etc. This will normally be followed by a password
Modem	(Modulator/demodulator) a device to allow conversion of bits into analogue electrical impulses for transmission over the telephone-type circuits, and vice versa, enables access to the Internet and remote working
Network password	Password used to give authorisation to access certain computer systems.
P.C.	**P**ersonnel **C**omputer
Security Systems	System that is in place to protect it from unauthorised use that adheres to the Reference Data Protection Act and Computer Misuse Act.
Software	Consists of programs, routines, procedures and their associated documentation, which can be implemented on a computer system.
Systems	Usually refer to individual applications e.g. Council Tax Benefits, Environmental Health, logged onto from the main log in. Can also refer to the computer operating system e.g. Windows, DOS or UNIX
Virus	A program hidden among legitimate software and loaded onto an unsuspecting users computer. When triggered i.e. running that program, the virus may cause damage to data on that computer.

10. Appendix 3 – Acknowledgement tear-off slip

Please sign the tear off slip to indicate that you have read, understood and will comply with the ICT Security Policy. This is to be returned to your line manager (or in the case of Councillors to the Head of ICT). These documents will be stored centrally within HR

PLEASE NOTE: Failure to comply may result in disciplinary action

---

ICT Security Policy [v2]

I have read and understood the Breckland Council ICT Security Policy v2 (July 2010010 issue).

I understand that non compliance may result in disciplinary action.

Name .....

Operational Group/Service Area .....

Date .....

Signature .....