Suffolk County Council

Acceptable Use of ICT Policy

Owner	**: Head of Information Management**
Document ID	**: ICT-PL-0003**
Version	**: 3.6**
Date	**: December 2015**

We will on request produce this Policy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.

DOCUMENT CONTROL

Changes History

Issue No	Date	Amended By	Summary of Changes
3.2	May 2011	Neal Scarff	Previous version
3.3	November 2013	Neal Scarff	Updates re use of Mobile Devices Abroad, DBS checks and use of home printers
3.4	May 2015	Neal Scarff, Philip Barbrook, Duncan Farley	Re-formatting & Updates
3.5	October 2015	Neal Scarff	Egress updates
3.6	December 2015	Neal Scarff	Unified Comms Updates

Authorisation (Responsible Owner)

Role	Name	Approval Date
Head of Information Management	Peter Knight	December 2015

Approval (Accountable Owner)

Role	Name	Approval Date
Senior Information Risk Owner	Chris Bally	December 2015

Reviewers (Consulted)

Role & Review Responsibilities	Name	Approval Date
Enterprise Architect	Philip Barbrook	December 2015
Policy & Compliance Manager	Neal Scarff	December 2015

Distribution List - Once authorised (Informed)

Name	Organisation
All Users	See Section 1.3.1 of the Policy

Review Period

Date Document to be Reviewed	By whom
December 2017	Head of Information Management

Table of Contents

1 INTRODUCTION

1.1 Purpose

1.1.1 The purpose of this policy is to:

- define and describe the acceptable use of ICT (Information and Communications Technology) for Suffolk County Council (SCC);
- minimise the risk to ICT facilities and the information contained in them and protect Councillors, employees and our partner organisations from litigation.

1.1.2 It is not the intention of this policy to impose restrictions that are contrary to the established culture of openness and trust, and Councillors' rights of access to information.

1.2 Background

1.2.1 The primary objectives of this policy are to:

- safeguard the integrity of data, ICT facilities and equipment;
- minimise the liability arising from the misuse of ICT facilities and equipment;
- protect the confidentiality of data and privacy of its users, to the extent required or allowed under law;
- maintain the availability of ICT facilities and equipment within the timeframe specified in Service Level Agreements.

1.3 Scope

1.3.1 This policy applies to the use of ICT facilities and equipment for which SCC is accountable and responsible. It is applicable to SCC Councillors, the employees of SCC, including temporary workers and agency staff, any partners, workers from voluntary groups, third parties and agents who SCC employees have authorised to access ICT facilities and equipment, including contractors and vendors with access to ICT facilities and equipment. For the purposes of this Policy all these individuals are referred to as 'user' or 'users'.

1.3.2 For the purposes of this Policy ICT equipment means any ICT device including, PC's, laptops, monitors, PDA's, tablets, mobile or smart phones, printers, scanners, photocopiers or mobile media (this is not an exhaustive list).

1.4 Linked/Other useful policies/procedures

1.4.1 This policy should be read in conjunction with the:

- Email Acceptable Use Policy;

- Password Management Policy;
- ICT Remote Working Policy;
- Role Based Access Control Policy;
- Clear Desk Policy;
- Software Policy;
- Removable Media Policy;
- Information Security Incident Management Policy;
- Information Security Policy;
- Freedom of Information Policy;
- Records Management & Information Handling Policy;
- Data Protection Policy;
- Protective Marking Policy;
- Social Media Policy;
- Use of ICT Portable Devices Policy;
- CCTV Policy;
- Web Conferencing Guide.

2 RESPONSIBILITIES

2.1 Suffolk County Council

2.1.1 **ICT Systems Ownership** - All ICT facilities are the property of SCC. This includes ICT equipment provided to users (including laptops and other mobile devices), software, operating systems, storage media and network accounts providing access to electronic mail and Internet services.

2.1.2 **Training** - SCC will train users in the Acceptable Use of ICT, including health and safety requirements under the display screen regulations 1992, Information Security, Protective Marking Awareness, PCI DSS and Data Protection, including when it is appropriate and permissible to share data.

Training for Councillors will be provided as part of the Councillors’ Learning and Development Programme.

2.1.3 **User Access to Networks** - SCC is responsible for approving and authorising user access to Council Networks, ICT facilities and equipment, and specific other secure networks (e.g. Public Services Network (PSN), Government Connect Secure Extranet (GCSx)).

For **Councillors**, approvals and authorisations will be provided by the Head of Scrutiny and Monitoring.

2.1.4 **User Access to Networks Administration** – IT is responsible for the administration for granting access to Council Networks, ICT facilities and equipment for users who have been approved and authorised by SCC managers and will maintain a central registry of all authorised users and assets. All authorised devices will have an asset security tag attached that relates back to the central register of assets.

For **Councillors**, approvals and authorisations will be provided by the Head of Scrutiny and Monitoring.

2.1.5 **Remote Access to Networks** - IT is responsible for the administration for granting users Remote Access to Council Networks for users who have been approved and authorised by SCC managers. The relevant documentation needs to be completed and signed-off by all parties prior to access. For more information please contact the IT Helpdesk.

For **Councillors**, approvals and authorisations will be provided by the Head of Scrutiny and Monitoring.

2.1.6 **Third Party Access to Networks** – IT is responsible for the administration for granting third-party access to Council Networks where users have been approved and authorised by SCC managers. The relevant documentation needs to be completed and signed-off by all parties prior to access. For more information please contact the IT Helpdesk.

2.1.7 **Third Party Access to Data** – IT is responsible for the administration for granting third-party access to data and data transfers where access and data transfers have been approved and authorised by the relevant SCC system/data owner and accountable person. The relevant documentation needs to be completed and signed-off by all parties prior to access. For more information please contact the IT Helpdesk.

2.1.8 **Information Security** - IT is responsible for appointing a manager who will coordinate and facilitate the Information Security programme in collaboration with partner organisations. This programme, which will be monitored, will include but not be limited to the following:

- Development and implementation of information security policies, standards, controls, procedures, and practices in order to protect ICT facilities and equipment;
- Development of information security training for system administrators;
- Establishment of a central repository for recording, tracking and resolving security-related incidents through collaboration with partner organisations.

2.1.9 **System or Account Misuse** - When a complaint of possible system or account misuse by an employee is reported, the validity of the incident will be reviewed according to the *Conduct and Capability Policy*. Incidents will be acknowledged and investigated in a timely manner. The Head of Audit Services will be appraised of each incident. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal.

When a complaint of possible system or account misuse by a **Councillor** is reported, the validity of the incident will be reviewed according to the *Members' Code of Conduct*. Incidents will be acknowledged and investigated in a timely manner. The Monitoring Officer will be appraised of each incident. In certain circumstances, breach of this policy may be considered a breach of the *Members' Code of Conduct* leading to action by the Standards Committee.

When a complaint of possible system or account misuse by any other user is reported, the validity of the incident will be reviewed in accordance with the background of the user under question. Incidents will be acknowledged and investigated in a timely manner. The Head of Audit Services will be appraised of each incident.

2.1.10 **Equipment Disposal** - Equipment disposal will be managed in accordance with the *SCC Environmental Management System and Procurement Regulations* and the *Waste Electrical & Electronic Equipment Directive (WEEE)*. Mobile Media (e.g. CD ROMS, DVDs) should be disposed of by way of shredding.

2.1.11 **Access to Work Applications** - IT is responsible for supporting ICT equipment and software provided to users relevant to Access to Work applications.

2.2 CIO Information Management Team

2.2.1 **Implementation and Monitoring of Policy** - The CIO Information Management Team has been tasked to implement this policy and monitor its effectiveness.

2.2.2 **Reported Breach of Information Security** - The CIO Information Management Team will manage the investigation of any reported breach of information security.

2.3 Managers

2.3.1 **Induction, Training and Support** - Managers are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them so as to implement this policy (see 2.4.1).

2.3.2 All line managers and those engaging third parties to act on behalf of the Council must ensure that their users are adequately trained and equipped to carry out their role efficiently and securely. All users, therefore, must undertake appropriate information security awareness training and regular updates in related statute and organisational policies and procedures as relevant for their role. This should be done as part of the induction process and recorded against an induction checklist to verify that this has been done. Additionally for employees line managers should use the probation period to ensure user awareness of the relevant policies and procedures.

2.3.3 The Council delivers online training modules about Information Security and the Council's policies. Line managers of new staff must ensure that new starters receive this training, understand it and complete it. In addition, line managers need to ensure that staff undertake regular refresher training as appropriate to their role.

2.3.4 Line managers need to make specific arrangements to include contractors or partners. The Council must ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their work, and to reduce the risk of human error.

2.3.5 In addition, employees who handle information carrying a protective marking of OFFICIAL-SENSITIVE data must be made aware of the impact of loss of such material through specific training e.g. PCI DSS.

2.3.6 The Monitoring Officer is responsible for ensuring that adequate induction and training is undertaken by Councillors and that support is provided to them so as to implement this policy.

2.3.7 **User Access** - Managers are responsible for:

- approving and authorising user access to Council Networks, ICT facilities and equipment, and specific other secure networks (e.g. Public Services Network (PSN), Government Connect Secure Extranet (GCSx));
- monitoring the subsequent use by the people they have authorised;
- notifying ICT to remove access promptly when the user leaves the organisation; and
- ensuring access permissions are reviewed and modified as required when their staff move to different roles within the organisation.

Prior to being provided with any access to ICT facilities, equipment and applications managers must ensure that the user has successfully completed any mandatory training and possesses all required documentary evidence (e.g. Baseline Personnel Security Standard, DBS).

Councillor User Access – Following their election, Councillors will be offered ICT equipment and access to Council Networks, and specific other secure networks (e.g. Public Services Network (PSN)), where these are required to enable them to fulfil their responsibilities as a Councillor.

The Head of Scrutiny and Monitoring is responsible for:

- approving and authorising this access;
- notifying ICT to remove access promptly when the Councillor's term of office ends; and

- ensuring access permissions are reviewed and modified as required if the Councillor’s role within the Council changes.

The Head of Scrutiny and Monitoring must ensure that the Councillor has successfully completed any mandatory training and possesses all required documentary evidence (e.g. Baseline Personnel Security Standard, DBS).

2.3.8 **User Access Suspension -** Managers are responsible for immediately requesting suspension of a user’s access to Council Networks, ICT facilities and equipment, specific other secure networks (e.g. Public Services Network (PSN), Government Connect Secure Extranet (GCSx)), ICT systems and applications where it is found that the user has not successfully completed any mandatory training or does not possess all required documentary evidence (e.g. Baseline Personnel Security Standard, DBS). Such requests should be made to the Policy & Compliance Team directly or via the IT Helpdesk.

Councillor User Access Suspension – The Head of Scrutiny and Monitoring is responsible for immediately requesting suspension of a Councillor’s access to Council Networks, ICT facilities and equipment, specific other secure networks (e.g. Public Services Network (PSN)), ICT systems and applications where it is found that the Councillor has not undertaken the necessary training, or does not possess the appropriate documentary evidence entitling them to access. Such requests should be made to the Policy & Compliance Team by the Head of Scrutiny and Monitoring.

2.3.9 **Changes in Personnel** - Managers are responsible for ensuring that information regarding changes in personnel is provided in a timely manner to avoid compromising the security of information, ICT facilities and equipment.

2.3.10 **Councillor Changes** – The Head of Scrutiny and Monitoring is responsible for ensuring that information regarding Councillor changes is provided in a timely manner to avoid compromising the security of information, ICT facilities and equipment.

2.4 Users

2.4.1 **User Awareness and Training -** All users should attend the appropriate training courses and ensure that they possess and supply all required documentary evidence (e.g. Baseline Personnel Security Standard, DBS). SCC delivers modular training to all users who have access to the council’s data and network. These training modules inform users of the requirements of the ICT Security Policies. All users must engage with this training and complete all mandatory and specific modules relevant to their roles. Line managers have a responsibility to support this training, and must raise with HR if any staff member does not, or cannot complete the training.

2.4.2 **User Understanding** – Users must understand and comply with the corporate commitments and information security measures associated with this *Acceptable Use of ICT Policy*.

2.4.3 **User Agreement** – By using the ICT equipment provided to them and by logging on to ICT systems, users agree to abide by this *Acceptable Use of ICT Policy* and other related policies.

2.4.4 **User Account Name and Password -** All users must have a unique user account name and password. Where a user works for more than one organisation they may be provided with a separate user account for each organisation. If a user moves from one organisation to another then they will be provided with a new user account. If a user moves from one directorate or department to another within the same organisation then they may be provided with a new user account dependent on the information security risk of keeping the original user account. The Policy & Compliance Team will provide final approval where appropriate.

2.4.5 **Access Authorisation** – Users must not connect, or attempt to connect, any ICT equipment provided to them to any network, or system; or access, or attempt to access, any network or system without prior explicit authorisation to do so.

2.4.6 **Access after 20:00** – Users must be aware that PC's will be shut down at 20:00 daily in accordance with the Council's Green Agenda. Users will receive an on-screen warning of the imminent shutdown and can continue working by then opting to stop the shutdown process.

2.4.7 **Breach of this Policy** - Staff found to be in breach of this policy may be disciplined in accordance with the *Conduct and Capability Policy*. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal.

Councillors found to be in breach of this policy may be deemed to have breached the *Members' Code of Conduct* and may lead to a referral to the Council's Monitoring Officer.

2.4.8 **Breach of Information Security** - Users must report all suspected breaches of information security to the CIO Information Management Team using the *Information Security Incident report form* via IT Self Service.

2.4.9 **Data Protection** - All users are expected to act in a responsible, ethical and lawful manner with the understanding that corporate electronic and manual information may be accessible to the public under the relevant information legislation. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design – nor to publish any defamatory content. Users and managers responsible for managing data should follow current *Data Quality Policies* and best practice. This includes specifying and taking appropriate measures to secure data from unauthorised access during normal working processes, in transit or when in storage. (See also the *Data* section)

2.4.10 **Authorised ICT Equipment** – Users must only attempt to access Council Networks from authorised ICT equipment and systems.

2.4.11 **PC & Laptop Connection to Council Networks** – **All** Council allocated PC's and laptops **must** be connected to Council Networks **at least once every 3 months, directly via a cable or the Council's wireless facility,** so as to ensure that anti-virus and security updates are applied. The **minimum** connection period via a cable or the Council's wireless facility is **4 hours**.

Note: Users using a Secure Network Connection (SNC) will be required to connect their PC or laptop to Council Networks as stated above.

2.4.12 **PC & Laptop Deactivation** - If a PC or Laptop has not been connected to Council Networks at least once in a 3 month period for the minimum connection period as stated in 2.4.11, it will be deactivated and users will not be able to access Council Networks using that device. Please contact the IT Helpdesk if you require assistance where the device has been deactivated.

2.4.13 **Authorised Location** – Users must only attempt to access the Public Services Network (PSN), or the Government Connect Secure Extranet (GCSx) from explicitly authorised locations.

2.4.14 **Movement of ICT Equipment** - Users must not move to a new location ICT equipment that is ordinarily fixed (e.g. PC base units, printers and monitors). Local audit trails detailing current locations must be maintained for mobile devices shared within a team (e.g. laptops and portable data storage devices).

2.4.15 **Mobile Devices** - Users allocated mobile devices (e.g. laptops, tablets, mobile or smart phone) must ensure that they are kept securely when not in use, or being transported and returned to ICT via their manager when they leave, or transfer to a role where the mobile device is no longer required within the organisation. The Council's insurance policies do not cover loss of equipment from unattended vehicles (see the *Remote Working Policy)*.

Councillors should return mobile devices to the Head of Scrutiny and Monitoring.

2.4.16 **Mobile or Smart Phones** – Council supplied mobile or smart phones are provided when necessary for the user to carry out their duties.

2.4.17 **Mobile Devices & Hands Free** – Mobile devices (e.g. mobile or smart phone) must only be connected to authorised hands free systems.

2.4.18 **Mobile Devices & Contact Data** – Users must not export any contact data from a mobile device (e.g. mobile or smart phone) to any other device, or system unless authorised to do so by ICT staff.

2.4.19 **Mobile Devices Use** – Users must not allow anyone, other than authorised ICT staff, to access an allocated mobile device (e.g. mobile or smart phone), or to use an authorised hands free system whilst the mobile device is connected.

2.4.20 **Legal Responsibility** - No user may use ICT facilities and equipment in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of SCC.

2.4.21 **Password and User Account Protection** - Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not log on to a machine using their password for another user to then use. Users must not under any circumstances reveal their password to ICT staff or anyone else. (See the *Password Management Policy*)

2.4.22 **Access to Another User's Personal Electronic Documents** - No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law. (See the *Email Acceptable Use Policy*) Personal electronic documents are those that are solely non business electronic documents.

2.4.23 **Passwords** - Users must choose passwords carefully and to comply with the *Password Management Policy*. All application passwords must be changed at least every 42 days (automatically forced where possible).

2.4.24 **Software** – Please refer to the *Software Policy*.

2.4.25 **Social Media** – Please refer to the *Social Media Policy*.

2.4.26 **Web Conferencing** – Please refer to the *Web Conferencing Guide*.

2.4.27 **Access to Data** - Users must not access, load or download any data on any ICT equipment without the knowledge, approval and authorisation of their manager and that of the owner and accountable person for the system the data originates from.

Councillors must not access, load or download any data on any ICT equipment without the knowledge, approval and authorisation of the owner and accountable person for the system the data originates from.

2.4.28 **Anti-Virus and Personal Firewall Software** - Network connected ICT equipment must have ICT approved anti-virus and personal firewall software installed, activated and functioning. Users may not turn off anti-virus and personal firewall software. All users of ICT facilities and equipment have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT facility or equipment. If ICT equipment is identified as being infected with a possible virus, Trojan or worm, steps will be taken to isolate it from the network immediately.

2.4.29 **ICT Security and Connection to Networks** - No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT facilities and equipment. No one may use ICT facilities and equipment to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. No one may make or attempt to make any unauthorised connection to the SCC network or connect any computer, network system or other ICT equipment to any of the SCC networks unless it has been supplied by or is managed by ICT. Access to networks will be monitored as allowed for by this policy and law (see 2.7.5).

2.4.30 **Wireless Connections** – Users are **not** permitted to connect any ICT equipment that has been supplied or is managed by ICT to an unsecured Wireless Network unless to enable a remote access session to the Councils network via the Secure Network Connection (SNC) service.

2.4.31 **Business Broadband Services provided by SCC** – Users are **only** permitted to connect ICT equipment that has been supplied or is managed by ICT to a Council Business Broadband Service (wireless or wired). This explicitly means that **no** personal equipment can be connected.

2.4.32 **Inappropriate Material** - No one may use ICT facilities and equipment to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a SCC account. (See the *Email Acceptable Use Policy*)

2.4.33 **Inappropriate Content** - The following content should not be created, accessed, or stored on any ICT facilities or equipment at any time:

- pornography and “top-shelf” adult content;
- material that gratuitously displays images of violence, injury or death;
- material that is likely to lead to the harassment of others;
- material that promotes intolerance and discrimination on grounds of age, disability, gender, gender reassignment, marriage and civil partnerships, pregnancy and maternity, race, religion or belief, sexual orientation.

- material relating to criminal activity, for example buying and selling illegal drugs;
- material relating to any other unlawful activity e.g. breach of copyright;
- material that may generate security risks and encourage computer misuse.

2.4.34 **Operational Exceptions -** There may be cases where users will, for operational reasons, require access to websites and other electronic data that would normally contravene this policy e.g. during investigations by Trading Standards, Audit Services, or ICT Investigation Teams. Assistant Directors and/or Strategic Information Agents must formally approve these operational exceptions.

Councillors requiring access to such websites must provide a reason for the request and approval must be given by the Head of Scrutiny and Monitoring.

The Policy & Compliance Team must be made aware of any such approvals using the *General Exceptions Request Form* via IT Self Service. The Policy & Compliance Team will provide final approval where appropriate. Users must only access websites and other electronic data for the approved business use.

2.4.35 **Accidental Access of Inappropriate Material or Content** - It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If users have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Policy & Compliance Team via the IT Helpdesk or IT Self Service. This may avoid problems later should monitoring systems be alerted to the content.

2.4.36 **Website Blocking** - The Council may block user access to various categories of websites on the Council networks, including download of content capability. This could be because the websites are not determined as appropriate for business use, or providing access could compromise the bandwidth of the Internet capability for essential business use, or that the content or download of content could pose a security threat to the Council Networks. If there is a business need to access or download content from a blocked website then this can be requested using the *General Exceptions Request Form* via IT Self Service providing a full business case for doing so. Please note that if ICT equipment is authorised to be connected directly to the internet then the Council may not be able to block user access to various categories of websites however 2.4.33 to 2.4.35 still apply.

Councillors requiring access to a blocked website must provide a reason for the request and approval must be given by the Head of Scrutiny and Monitoring.

The Policy & Compliance Team must be made aware of any such requests and approvals using the *General Exceptions Request Form* via IT Self Service. The Policy & Compliance Team will provide final approval where appropriate. In these cases users must not access any areas of the site or download content that is not an approved legitimate business need.

2.4.37 **Website Appropriate Access -** There may be circumstances where a website that would normally be blocked may not be because there is a legitimate business need to access areas of the website, or download appropriate content. In these cases users must not access any areas of the site or download content for which there is not a legitimate business need.

2.4.38 **Standard Desktop -** Screensavers and desktop wallpaper must match the corporate standard (as supplied by IT as standard build). The IT Helpdesk is authorised to revert screensavers, desktop wallpaper, or any other settings, to the corporate standard if found to be non-compliant.

2.5 Mobile & Home Working

2.5.1 See also paragraph 2.1.5.

2.5.2 **Designated Mobile and Home Workers** - Managers should ensure that designated Mobile and Home Workers are provided with the relevant equipment to allow for mobile and home working.

2.5.3 **SCC Webmail Service** - Users of the SCC Webmail Service (Outlook Web Access) must ensure that any ICT equipment accessing this service has antivirus and local firewall software installed, enabled and regularly updated. The SCC Webmail Service allows users to access their emails whilst away from the office and to view any attachments. Users are not authorised to save to local ICT equipment, even temporarily so that they can then work on it, any email, document or information that is, or would be, classified as OFFICIAL-SENSITIVE or above (see also the *Protective Marking Policy*).

2.5.4 **Secure Network Connection** - ICT provides support for the initial configuration of a Laptop for allowing the Secure Network Connection (SNC) to enable mobile and home working. However, the broadband, wireless and wired connectivity is not supported by ICT.

2.5.5 **Working Outside the UK** – Portable electronic devices and removable media are allowed to be transported and used outside the United Kingdom under certain conditions. The *Use of ICT Portable Devices Policy* provides further details and a list of permitted countries.

2.6 ‘Tokens’

2.6.1 **Security of Token** - Users allocated a ‘Token’ (a small device that provides a randomly generated number for use as a password) to access ICT facilities must ensure that the ‘Token’ is kept securely at all times and report if it is lost or damaged at the first opportunity to the IT Helpdesk. If a replacement has to be provided then charges will be incurred.

2.6.2 **Return of Token** - Users must ensure that the 'Token' is returned promptly to their line manager if they leave SCC, or change roles and it is no longer required. Managers must ensure that the 'Token' is returned promptly to ICT.

2.7 Personal Use and Privacy

2.7.1 **Limitations of Personal Use** - In the course of normal operations, ICT facilities and equipment are only to be used for business purposes. SCC permits the personal use of ICT facilities and equipment by authorised users subject to the following limitations:

- Personal use must be in the user's own time and must not impact upon business efficiency or costs;
- The level of personal use must be reasonable and not detrimental to the main purpose for which the ICT facilities and equipment are provided;
- Personal use must not be of a commercial or profit-making nature;
- Personal use must not be of a nature that competes with the business of the Council or its partners or conflicts with a user's obligations;
- Personal use must not conflict with the *Code Of Conduct* or a **Councillor's** obligations under the *Members' Code of Conduct*.

2.7.2 **Examples of Acceptable Personal Use** - Examples of acceptable personal use of ICT include online banking, shopping, learning activities, access to news and weather websites and the use of MS Office and email for personal organisation or charitable and other non-profit making activities. (See also *Email Acceptable Use Policy*)

2.7.3 **Sound or Image Files** - File formats associated with sound or images (e.g. JPEG, WAV, MP3) must not be stored on SCC servers or local hard drives for non-work purposes. ICT will remove inappropriate files if found unless they are required for evidence relating to a disciplinary issue. (See also *Email Acceptable Use Policy*)

2.7.4 **Inappropriate Content** - Personal use of the Internet must not involve attempting to access the categories of content described in section 2.4.33. If you are connecting ICT equipment to any other network than the SCC network then this policy still applies.

2.7.5 **Recording and Inspecting Information** - Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, SCC may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated, or is violating this policy, or any guidelines, or procedures established to implement this policy;

- An account appears to be engaged in unusual or unusually excessive activity;
- It is necessary to do so to protect the integrity, security, or functionality of ICT facilities and equipment or to protect SCC or its partners from liability;
- Establishing the existence of facts relevant to the business;
- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities and equipment;
- Preventing or detecting crime;
- Investigating or detecting unauthorised use of ICT facilities and equipment;
- Ensuring effective operation of ICT facilities and equipment;
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened);
- It is otherwise permitted or required by law.

2.7.6 **Monitoring** - Any necessary monitoring will be carried out in accordance with the Information Commissioner's Office (ICO) *Code of Best Practice on Monitoring Employees*.

2.7.7 **Monitoring of PSN, GSi and/or GCSx** – Users must acknowledge that their use of the Public Services Network, Government Secure Intranet (GSi) and/or the Government Connect Secure Extranet (GCSx) may be monitored and/or recorded for lawful purposes.

2.7.8 **Violation of this Policy** - Where an individual has reasonable cause to believe that another user has violated, or is violating this policy, or any guidelines, or procedures established to implement this policy then they shall in the first instance inform a Senior Manager who may refer the matter on to the HR Professional Services Team via the HR Helpdesk for investigation under the *Conduct and Capability Policy* as in 2.1.10. If the HR Professional Services Team advise the Senior Manager that use needs to be checked in accordance with 2.7.5 then the Senior Manager should refer this to the Policy & Compliance Team directly or via the IT Helpdesk. In these circumstances the checks may necessitate the immediate suspension of the user's access to relevant Council Networks, ICT facilities and equipment, ICT systems and applications in order that any potential evidence is not compromised.

Where an individual has reasonable cause to believe that a **Councillor** has violated, or is violating this policy, or any guidelines, or procedures established to implement this policy then they shall in the first instance inform a Senior Manager who should refer the matter on to the Head of Scrutiny and Monitoring for investigation. If the Head of Scrutiny and Monitoring advises that use needs to be checked in accordance with 2.7.5 then they should refer this to the Policy & Compliance Team. In these circumstances the checks may necessitate the immediate suspension of the Councillor's access to relevant Council Networks, ICT facilities and equipment, ICT systems and applications in order that any potential evidence is not compromised.

2.8 Data

2.8.1 **Managing Data -** Managers responsible for managing data should follow current *SCC Data Quality policies* and UK Government best practice as described by the Cabinet Office in the *Information Assurance Policy guidelines*. This includes specifying and taking appropriate measures to secure data from unauthorised access during normal working processes, in transit, when in storage or in the possession of third parties and ensuring that the correct protective marking is shown (see *Protective Marking Policy*). Current policy guidelines can be found at: http://www.cabinetoffice.gov.uk/ogcio/isa.aspx

Councillors are responsible for managing the data that they hold. They have the same responsibility as Managers to ensure that this data is handled securely and should follow the policies and guidance described above.

2.8.2 **'Sensitive' or Protectively Marked Data** - Where the user is accessing a system showing 'sensitive' or Protectively Marked data then the screen must not be easily readable by anyone other than the logged-in user. Workstations and screens shall be arranged to ensure that the screen is facing away from the line of sight of any visitors. Managers should ensure that 'Restricted access' areas are created in an open plan environment to protect sensitive data from being viewed by others and to emphasise the need for privacy (see also *Protective Marking Policy*).

2.8.3 **User Profiles** – User profiles (icons on your desktop plus my documents, if used) shall not exceed 100MB in size. There may be business cases where, for operational reasons, a profile needs to exceed 100MB. Assistant Directors and/or Strategic Information Agents must formally approve each business case and keep to a minimum any operational exceptions. The Policy & Compliance Team must be made aware of any such approvals via ICT Self Service.

For **Councillors**, approvals and authorisations will be provided by the Head of Scrutiny and Monitoring.

The Policy & Compliance Team will provide final approval where appropriate.

2.8.4 **Individual Folders** - Individual folders, where allocated to users for individual use, shall not exceed 100MB in size. There may be business cases where, for operational reasons, folders need to exceed 100MB. Assistant Directors and/or Strategic Information Agents must formally approve each business case and keep to a minimum any operational exceptions. The Policy & Compliance Team must be made aware of any such approvals via ICT Self Service.

For **Councillors**, approvals and authorisations will be provided by the Head of Scrutiny and Monitoring.

The Policy & Compliance Team will provide final approval where appropriate.

2.8.5 **Personal Documents and Folders -** Personal documents and folders regarded as "personal" must be clearly titled to reduce the risk of administrators inadvertently viewing private, non-work documents. Personal documents and folders must be deleted from SCC systems as soon as possible.

2.8.6 **Data and Record Storage** - Important data and corporate records may not be stored on local hard drives or private folders but must be organised and managed according to The Suffolk File Plan on shared servers in compliance with the *Freedom of Information Policy*. Corporate records include the following:

- policy statements and implementation plans;
- directives, decisions & approvals for a course of action;
- documents that initiate, authorise, change or complete business transactions;
- briefing papers, reports & background papers;
- agendas and minutes of meetings;
- project documentation;
- customer transaction records.

2.8.7 **Records Retention** - According to their content, electronic records will be kept for a period defined in the corporate *Records Retention Guidelines* detailed within the Suffolk File Plan. The Information Compliance Helpdesk can advise on long-term digital preservation strategies. All other non-records must be deleted promptly i.e. within 3 months.

2.8.8 **Payment Card Data** - You must **not** store or save Credit or Debit Card numbers on any Council ICT Resource. **This includes storing the information in applications, email, spreadsheets, any type of document, database or computer file.** Credit or Debit card numbers include the 'long' card/account number (PAN), the Card Security Code (CSC – number printed on reverse of card) and the PIN number. The exception to this is when Debit or Credit card payments are made using an authorised Council secure payment service.

2.8.9 **Debit or Credit Card Payments** - If you process Credit or Debit card payments in the course of your work, you must do this in accordance with the Payment Card Industry Data Security Standard (PCI DSS), your terminal Operating Manual and any job-specific guidance on handling payment card data. Your line manager can provide you with job-specific guidance on handling payment card data.

2.8.10 **Debit or Credit Card Payments via the Internet** - Users must only use authorised ICT equipment that is PCI DSS compliant when accessing the internet in order to process debit or credit card payments.

2.8.11 **Folder and File Permissions** - Managers are responsible for ensuring that all folder and file permissions are appropriate to the information content and in line with the *Protective Marking Policy*.

For **Councillors**, the Head of Scrutiny and Monitoring is responsible for ensuring that all folder and file permissions are appropriate to the information content and in line with the *Protective Marking Policy*.

2.8.12 **Storage and Integrity of Corporate Records** - Any corporate records that are *already* held on portable media must be stored in appropriate environmental conditions and periodically checked for integrity – for further advice contact the Information Compliance Helpdesk.

2.8.13 **Printed Material** – Users must securely store or destroy any printed material.

2.8.14 **Movement of Data and Records** – Users must not remove information (data and records both electronic and paper) from Council premises without appropriate approval.

2.8.15 **Internal Data Exchange** – Where a non business as usual data transfer is required internally between service areas then an Internal Data Exchange Agreement needs to be created, completed and signed-off by all parties prior to data transfer.

2.8.16 **Third Party Code of Connections and Access to Data** - IT is responsible for the administration for granting transfer of data to third-parties where data transfers have been approved and authorised by the relevant SCC system/data owner and accountable person. This includes maintaining an audit trail for the data extract throughout its lifecycle (from creation to delivery/disposal). The relevant documentation needs to be completed and signed-off by all parties prior to access. For more information please contact the IT Helpdesk.

2.8.17 **GCSx Data** - Users of the Government Connect Secure Extranet (GCSx) must:

- not transmit information via the GCSx that they know, suspect or have been advised is of a higher level of sensitivity than their GCSx domain is designed to carry;
- not transmit information via the GCSx that they know or suspect to be unacceptable within the context and purpose for which it is being communicated;
- not make false claims or denials relating to their use of the GCSx (e.g. falsely denying that an e-mail had been sent or received);
- protect any sensitive or not protectively marked material sent, received, stored or processed by them via the GCSx to the same level as they would paper copies of similar material;
- appropriately label information up to OFFICIAL-SENSITIVE sent via the GCSx (see also *Protective Marking Policy*);

- not send OFFICIAL-SENSITIVE information over public networks such as the Internet unless encrypted (see also *Protective Marking Policy*);
- always check that the recipients of e-mail messages are correct so that potentially sensitive or OFFICIAL-SENSITIVE information is not accidentally released into the public domain;
- not auto-forward email from their GCSx account to any other non-GCSx email account;
- not forward or disclose any sensitive or OFFICIAL-SENSITIVE material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel;
- seek to prevent inadvertent disclosure of sensitive or OFFICIAL-SENSITIVE information by avoiding being overlooked when working, by taking care when printing information received via GCSx (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted.

2.9 Remote Control Software

2.9.1 **Authorisation of Use of Remote Control Software** - Users of ICT facilities and equipment must not attempt to use remote control software without prior authorisation being provided by the Policy & Compliance Team.

2.9.2 **Use of Remote Control Software** - Authorised users must only use remote control software to connect and take control of ICT equipment (e.g. PC or laptop) remotely for helpdesk approved support and training purposes. Relevant documentation is required to be completed.

2.9.3 **Third Party Use of Remote Control Software** - Authorised third party users must only use remote control software to connect and take control of ICT equipment (e.g. PC or laptop) remotely for approved support and training purposes. The third party user will be supervised at all times during the connection session by a Council supervisor. Failure to comply with instructions or commands from the Council supervisor of the connection session will result in immediate disconnection. Relevant documentation is required to be completed for **each** individual connection session.

2.9.4 **Permission of Use** - Where the authorised user is to connect and take control of ICT equipment during a user’s live session then they must seek permission from the user prior to connecting.

2.10 Accessing Folders and Mailboxes of Users

2.10.1 **Access to Another User’s Folders or Email Mailbox** - Do not attempt to gain access to any other user’s folders or email mailbox without their permission.

2.10.2 **Legitimate Access to Another User’s Email Mailbox** - For legitimate access to mailboxes of users refer to the *Email Acceptable Use Policy*.

2.10.3 **Access to Another User’s Folders where the User is Absent and Granted Permission** - Where the user is absent (e.g. due to sickness), has granted permission to access their folders however is unable to set this up themselves, the set up can be requested via ICT Self Service. The request must be from the line manager of the person requiring access detailing the business need to do so. If the line manager is the person who is absent then the request needs to be from the next higher level manager. Managers should be aware that access would be time limited and strictly limited to business folders and files. The Policy & Compliance Team will provide final approval where appropriate.

For **Councillors**, approvals and authorisations will be provided by the Head of Scrutiny and Monitoring and notified to the Policy & Compliance Team.

2.10.4 **Access to Another User’s Folders where the User is Absent and is Unable to Grant Permission** - Where the user is absent and unable to provide permission to access their folders do not attempt to gain access without the express permission of the Policy & Compliance Team (available via ICT Self Service). Such requests should be from the line manager of the person requiring access detailing the business need to do so. If the line manager is the person who is absent then the request needs to be from the next higher level manager. Managers should be aware that such permission would only be granted in the last resort in the interests of business continuity, that access would be time limited and strictly limited to business folders and files. The Policy & Compliance Team will provide final approval where appropriate.

For **Councillors**, approvals and authorisations will be provided by the Head of Scrutiny and Monitoring and notified to the Policy & Compliance Team.

2.10.5 **Access to Another User’s Folders where the User has Changed Roles or Leaves the Employment of SCC** - Where the user changes roles or leaves the employment of SCC do not attempt to gain access to their folders without the express permission of the Policy & Compliance Team (available via ICT Self Service). Such requests should be from the line manager of the person requiring access detailing the business need to do so. If the line manager is the person who is changing roles or leaving then the request needs to be from the next higher level manager. Managers should be aware that such permission would only be granted in the last resort in the interests of business continuity, that access would be time limited and strictly limited to business folders and files. The Policy & Compliance Team will provide final approval where appropriate.

For **Councillors**, approvals and authorisations will be provided by the Head of Scrutiny and Monitoring and notified to the Policy & Compliance Team.

2.11 Managing Personnel Changes

2.11.1 **Transfer of Electronic Records where a User Changes Role or is Moving from one Organisation to Another or is Leaving the Employment of SCC** – Users must ensure that all electronic records in private folders or mailboxes are transferred to their manager if changing roles within SCC or moving from one Organisation to another and the records are no longer required for the new role, or if leaving the employment of SCC. All personal files and messages must be removed from hard drives and private folders. (See also the *Email Acceptable Use Policy*)

2.11.2 **Hand Back of Equipment where a User Changes Role or is Leaving the Employment of SCC** – Users must ensure that all equipment, including laptops, 'tokens' and storage devices, is handed back promptly to their line manager if they leave SCC, or change role within SCC and the equipment is no longer required for the new role. Managers must ensure that they do not reissue the equipment to any other user and that it is returned promptly to ICT.

2.11.3 **Informing ICT that a User Leaves SCC** - If a user leaves SCC, it is the manager's responsibility to ensure that ICT is informed immediately by logging a *Delete User Account* request via ICT Self Service so that they revoke access rights and shut down the account as soon as the user has left. For security purposes, private folders will be deleted 3 months after the departure of the user.

2.11.4 **Informing ICT that a User Changes Role Within SCC** - If a user changes role within SCC, it is the manager's responsibility to ensure that ICT is informed immediately by logging an *Amend User Account* request via ICT Self Service.

2.11.5 **Informing ICT of a New User** - If a user starts work for SCC, it is the manager's responsibility to ensure that ICT is informed immediately by logging a *New User Account* request via ICT Self Service.

2.11.6 **Informing ICT that a User's Account should be Suspended** - If a user's account is required to be suspended, for any reason, it is the senior manager's responsibility to ensure that the Policy & Compliance Team are contacted detailing the business case for the account suspension. The Policy & Compliance Team will provide final approval where appropriate.

2.11.7 **Informing ICT that a User is leaving the Employment of SCC quickly or on Discretionary Leave** - If a user is leaving the employment of SCC quickly (e.g. due to redundancy), or on discretionary leave, and the user account is required to be suspended and permissions removed due to potential information security/integrity risks, it is the Assistant Director's responsibility to ensure that the Policy &

Compliance Team are contacted immediately. It is the Assistant Director's responsibility to ensure that any ICT equipment that the user was allocated and is no longer required (e.g. laptop, 'token', mobile or smart phone) is collected prior to the user leaving and handed back to ICT.

2.12 Managing Councillor Changes

2.12.1 **Transfer of Electronic Records where a Councillor's Role Changes Within the Council or their Term of Office Ends** - Councillors must ensure that all electronic records in private folders or mailboxes are transferred to the Head of Scrutiny and Monitoring if the Councillor's term of office ends, or if their role changes within the Council and the records are no longer requires for the new role. All personal files and messages must be removed from hard drives and private folders. (See also the *Email Acceptable Use Policy*)

2.12.2 **Hand Back of Equipment where a Councillor's Role Changes Within the Council or their Term of Office Ends** - Councillors must ensure that all equipment, including PCs, laptops, 'tokens' and storage devices, is handed back promptly to the Head of Scrutiny and Monitoring if the Councillor's term of office ends, or if their role changes within the Council and the equipment is no longer required for their responsibilities as a Councillor.

2.12.3 **Informing ICT when a Councillor's Term of Office Ends** - The Head of Scrutiny and Monitoring is responsible for ensuring that ICT is informed immediately when a Councillor's term of office ends, by logging a *Delete User Account* request via ICT Self Service, so that they revoke access rights and shut down the account as soon as the term of office ends. For security purposes, private folders will be deleted 3 months after the departure of the Councillor.

2.12.4 **Informing ICT if a Councillor's Role Changes Within the Council** - The Head of Scrutiny and Monitoring is responsible for ensuring that ICT is informed immediately if a Councillor's role changes within the Council, by logging an *Amend User Account* request via ICT Self Service.

2.12.5 **Informing ICT of a New Councillor** - The Head of Scrutiny and Monitoring is responsible for ensuring that ICT is informed immediately of a new Councillor, by logging a *New User Account* request via ICT Self Service.

2.12.6 **Informing ICT that a Councillor's User Account should be Suspended** - If a Councillor's user account is required to be suspended, for any reason, the Head of Scrutiny and Monitoring is responsible to ensure that Policy & Compliance Team are contacted detailing the business case for the account suspension. The Policy & Compliance Team will provide final approval where appropriate.

3 REVIEW OF THE POLICY

3.1 Policy Review

3.1.1 This policy will be reviewed every two years, or when any other significant change impacts upon the policy. Comments on the policy, from both employees and members of the public, are therefore welcome and can be addressed to:

Information Management
Suffolk County Council
Constantine House
Constantine Road
Ipswich
Suffolk
IP1 2DH

4 FURTHER ADVICE

For further advice on this policy, please contact:
Your Strategic Information Agent, or

CIO Information Management Information.Management@suffolk.gov.uk