ICT Acceptable Use Policy

January 2019 (proposed date)

Summary Sheet

Document Information

Protective marking (Unclassified / Restricted Circulation / Confidential)	Unclassified
Ref	Acceptable Use ICT
Document Purpose	To ensure all users of Sefton's ICT are aware of guidance around acceptable use
Document status (Draft / Active)	Draft
Partners (If applicable)	N/A
Date document came into force	TBC
Date of next review	December 2019
Owner (Service Area)	Sefton Council – ICT Client Team
Location of original (Owner job title / contact details)	Helen Spreadbury
Authorised by (Committee/Cabinet)	Audit and Governance Committee

Document History

Version	Date	Author	Notes on revisions
0.1	27/09/2018	H Spreadbury	Draft
0.2	11/10/2018	H Spreadbury	Amendments made following consultation with IMG
0.3	15/10/2018	H Spreadbury	Further amendments made following consultation with HR and Agilisys
1	06/11/2018	H Spreadbury	Final draft following feedback from IMG

Further documentation and supporting material can be found –a link to appropriate web page will be inserted here before release

Introduction

The purpose of this document is to ensure that all Users of Sefton Council's ICT (Information Communications Technology) Services feel confident in the use of ICT to complete their work. The aim of this policy document is to describe in plain English what is acceptable activity to ensure the security of Sefton's ICT network, to protect the disclosure of information and ensure we can prevent, as far as possible, cyber-attack or cybercrime.

The increasing use of Information and Communication Technology and the development of information strategies to support the process of providing effective services make it necessary to take appropriate action to ensure that these systems are developed, operated and maintained in a safe and secure manner.

Whilst the aim is to provide facilities for employees to use freely in pursuit of their job there are, however, management and legal issues, which should be borne in mind to ensure the effective and appropriate use of information technology.

Scope

This document applies to all authorised users of Sefton's ICT systems; including; council employees, members, contractors, consultants, commissioned service providers and organisations that connect to or support any part of the IT Infrastructure

Individual Responsibilities

- All Elected Members must accept responsibility for maintaining ICT standards within the organisation.
- All Managers must accept responsibility for initiating, implementing and maintaining ICT standards within the organisation.
- All non-managerial employees must accept responsibility for maintaining standards by conforming to those controls, which are applicable to them.
- The ICT Client Team, supported by Agilisys, is responsible for implementation of technical security solutions to protect the network

How to Use this document

This document outlines what Sefton deems to be acceptable and unacceptable use of ICT, all colleagues as defined within the scope of this document must comply with this policy failure to do so may lead to disciplinary action.

If you do not understand the definitions and guidance in this document please do not hesitate to seek advice from either your manager, The ICT Client Team or the IT Helpdesk.

User Accounts and Passwords

Access to Sefton Council's ICT systems and Information must be adequately protected. Whilst different business applications have varying security requirements, these individual requirements must be identified through risk assessments that will 'control the access' to the ICT systems and filing cabinets where the information is held in paper form.

Management Responsibilities

- Managers must ensure that all staff within their team have access rights to systems and IT services that are commensurate with the tasks they are expected to perform

- All staff must have unique login that is not shared with or disclosed to any other users along with an associated unique password that is requested at each new login

- Employees must not make copies of computer software owned by the Council for private use

- User's access rights must be reviewed at regular intervals by their manager to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

- Managers must ensure that all computer software and hardware is purchased via the ICT Client team, under no circumstances should any free of charge evaluation software be installed without prior approval from the ICT client team

- All authorised users are required to comply with the Movers and Leavers Policy document found in Appendix A

1. IT Device Management

As a principle, and to ensure value for money, there will be no more than one workstation asset allocated per user (desktop, laptop or thin client) In exceptional cases staff requiring multiple assets must provide a business case (signed by Head of Service) to the ICT Client team before an additional device will be purchased.

How you should use your device (key principles)

- All devices directly connected to the Sefton MBC Network (wired, wireless or access via VPN) must be approved, deployed and supported by the ICT Managed Service Provider
- The installation of any software and any required local configuration is managed and supported by the ICT Managed Service Provider
- All devices are owned by Sefton MBC
- All mobile end user devices must be assigned a named individual within a team
- If a person moves role within the organisation the device remains with the leavers team for reallocation to the new postholder, in cases where there is no new postholder it must be returned to the ICT Managed Service Provider.
- All fixed desktops must be assigned to the departmental manager for that area
- All devices must be recorded within the departmental asset register
- When a device is no longer in use then the device must be returned to the ICT Managed Service provider
- All devices must be listed within the team's equipment inventory

Things you must not do

- Connect any personal devices to the corporate network – Bring your Own Device (BYOD) is not permitted
- Do not move or install devices without the support of ICT, all requests for installation, moves or changes to any device must be logged through the ICT Service Desk
- Do note dispose or reallocate any device without logging a call with the ICT Service Desk, any disposals must comply with WEEE Regulations 2017

2. User network and Applications Accounts

- Always use your own personal Sefton Council account to carry out your work
- Only use your administration account to carry daily specific system administrator duties assigned to you by your manager (if relevant)
- **Always use CTRL ALT DEL to lock your machine when unattended**
- Follow the password policy below

Choosing Passwords

Passwords are an important aspect of Sefton's ICT security. They are the front line of protection for user accounts.

A poorly chosen password may result in the compromise of Sefton's entire network. All employees, temporary workers, contractors, consultants and 3rd parties that have access to the IT systems must adhere to the password Mandatory Principles defined below to protect the security of the network, protect data integrity, and protect computer systems.

Individual users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. Report any suspicions of your password being compromised to the ICT Service Desk.

Things you must not do

- Never write passwords down
- Never send a password through email
- Never include a password in a non-encrypted stored document
- Never tell anyone your password or hint at the format of your password
- Never use your network password on an account over the internet which does not have a secure login, Secure web pages have addresses that start with https://
- Don't use common acronyms as part of your password
- Don't use spaces, common words or reverse spelling of words in part of your password
- Don't use names of people or places as part of your password
- Don't use parts of your login name in your password
- Don't use parts of numbers easily remembered such as phone numbers, NI numbers or street address
- Never let someone see you type your password

3. One Drive and SharePoint

Access to OneDrive for Business is from a managed Sefton Council **Windows 10** device or a managed mobile device only.

OneDrive for Business is your personal area on the cloud, confidential to you, previously known as your H:/. OneDrive for Business requires an Office 365 license, once employment ends this data will be accessible to the user's manager and will then be removed in line with the data retention policy, please refer to Appendix B

Sharepoint - a web-based collaborative platform that integrates with MS Office, used for sharing documents, this is where you will find all the documents migrated from your old G:/ or team drive or Microsoft Shares.

How you should use One Drive for Business and SharePoint

- All data stored in OneDrive for Business should be relevant to the user's role
- All data that needs to be shared across teams/groups must be stored in Share Point
- Data should be stored in line with the retention schedule and deleted when no longer required
- The sharing of files to third parties is permitted however this should only be done for valid business purpose, and approved by ICT Client and basic configuration supported by the ICT Service Desk

Things you must not do

- Personal data must not be kept in OneDrive for Business
- Personal/Copyright Pictures must not be stored in OneDrive for Business or Sharepoint
- Personal/Copyright Video's must not be stored in OneDrive for business or Sharepoint
- Any pictures, music or videos that are stored will be deemed to be property of Sefton Council

4. Internet Acceptable Use Policy.

The Council recognises that it is not practical to define precise rules that cover the full range of Internet activities available and in general, it is adherence to the spirit and essence of the policy that will allow the Council as a whole, and employees in person, to productively benefit from access to this powerful technology.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Sefton Council and may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory and internal policy requirements.

What you should use your Council Internet account for

Your Council Internet account should be used in accordance with this policy to access anything in pursuance of your work including:

- Access to and/or provision of information.
- Research
- Electronic commerce (e.g. purchasing equipment for the Council)
- Supported council applications which are hosted externally by the supplier
- Personal use in your own time (ie: during your lunchbreak), any personal use must not include any activity listed in the section below

The Council is not however responsible for any personal transactions you enter, for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the Council protected against, any claims, damages,

losses or the like which might arise from your transaction for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you purchase personal goods or services via the Council's Internet service, you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.

You should ensure that personal goods and services purchased are not delivered to Council property, rather, they should be delivered to your home or other personal address.

The Council is not responsible for any losses or issues relating to personal use of the Council's internet facility.

If you are in any doubt about how you may make personal use of the system you are advised not to do so.

Things you must not do

- Browse non-work sites during working hours
- Leave open live internet feeds to collect news, sports updates or to download images, video or audio streams for none work purposes
- Download any copyrighted material without the owner's permission
- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text /image messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business.
- Download any software used for hacking or cracking passwords
- Make repeated attempts to access any sites automatically blocked by the Council's filtering software

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

5. Email Acceptable Use Policy

The email system is provided to allow electronic communication in pursuance of Council business between Elected Members, Council employees, individual Council service users and external organisations. All email sent and received via Sefton Council is owned by the council and should not be deemed personal. The Council will monitor your email account usage may access your email content. Be aware that Sefton MBC may be required to disclose your emails or responses to them to third

parties for legal reasons, which may include requests made under the GDPR or Freedom of Information.

How you should use your email (key principles)

- Communication in connection with Sefton Council's business
- Users must exercise due care when writing an email to ensure that their message maintains the standards of professionalism the Sefton Council expects of their position
- Users should not make statements on their own behalf or on behalf of the Sefton Council that do or may defame, libel or damage the reputation of Sefton Council or any person
- Limited personal use of email is allowed provided it is kept to a reasonable level, does not interfere with a user's performance in carrying out their duties, does not have a negative impact on Sefton Council in any way, is lawful and adheres to the principles contained within this email Policy.
- Sefton Council email / public folders and shared mailboxes not accessed (e.g. opened content) for longer than 30 days will be disabled
- Sefton Council email / public folders and shared mailboxes not accessed for longer than 90 days will be deleted except where otherwise directed by the relevant manager ie: for long term sickness, maternity or direct instruction from HR, see Appendix A
- All Sefton Council email / public folders and shared mailboxes must have an owner and if an owner leaves it must be reassigned or the mailbox will also be removed in accordance with policies above.
- The Sefton Council ICT Division does not archive leavers information unless formally requested and approved by a manager or HR.
- Sefton Council reserves the right to monitor and/or record individual email use for lawful business purposes. Users should therefore have no expectation of privacy whilst using Sefton Council equipment for the purposes of communicating via email
- The contents of all email attachments, inbound and outbound, are scanned electronically to help implement this Mandatory Policy against the acceptable use policy and to prevent malware
- Individual users are responsible for the day-to-day house-keeping of their account and must minimise their mailbox space.

Things you must not do

- Use the Council's email system to facilitate or operate any business/ commercial activity, other than that of the Council.
- Send business related email to large distribution groups without the permission of the ICT Client Team
- **Email confidential, sensitive or personally identifiable information to other people (either internal or external) without ensuring that the data is secured and that the authority has the legal power or explicit consent to do so**
- Provide your work email address as contact details to sites you have accessed for non-work purposes
- Use personal web-based email from your work equipment ie: Google mail

- Send files with non-business-related attachments (ie compressed files, video streams, executable code, video or audio streams or graphical images)
- Email must only be accessed via the user's personal user account and users must not attempt to use another user's account without their prior expressed permission, but an individual's email may be accessed by an authorised Sefton Council colleague or manager once a user has left the Sefton Council or where it has been approved by the Head of HR
- Except where it is strictly and necessarily required for your work (for example, corporate advertising, IT audit activity or other investigation), you must not create, download, access, display, transmit or engage in the following:

    - full videos or clips
    - photographic or cartoon images
    - chain letters
    - jokes or 'joke' chains
    - conversational email
    - harassing or bullying content
    - entertainment software
    - other non-work related software
    - advertisements
    - global emails (see paragraph 13 below)
    - game
    - gambling

- Again, except where it is strictly necessary and required for your work (as defined above) you must not create, download, access, display, transmit or engage in the following

    - material that is obscene, offensive, sexually explicit, pornographic, racist, sexist, ageist, defamatory, hateful, or homophobic in nature, incites or depicts violence, or describes techniques for criminal or terrorist acts
    - derogatory remarks or express derogatory opinions regarding the Council, its Officers or Members or communicate extreme views that could be to the detriment of the Council or its reputation or bring the Council into disrepute

If you receive an unsolicited "unsuitable" email please inform your manager, and notify the ICT Service Desk.

6. Telephones

For the purpose of this policy the term 'Phones' refers to Council landlines and mobile telephony devices, including pool phones. Users are expected to exercise due care when making telephone calls and using mobile messaging, to ensure that they maintain the standards of professionalism the Council expects of their position. Managers have the responsibility to inform the ICT Service Desk when a mobile phone is no longer required, e.g. a member of staff has left, and the phone is not being passed on, so that the contract can be cancelled.

Sefton reserves the right to monitor and record/log individuals' use of the mobile device systems for its lawful business purposes. Sefton's employees, secondees and workers must not expect privacy whilst using Council equipment for the purposes of communicating. Sefton MBC may be required to disclose voice recordings to third parties for legal reasons, which may include requests made under the GDPR or Freedom of Information Act.

How you should use your Telephone (key principles)

- In connection with normal business
- Use of personal mobile phones in work for short conversations/messages provided it is kept to a reasonable level, does not interfere with a user's performance in carrying out their duties, does not have a negative impact on Sefton Council in any way, is lawful and adheres to the principles contained within this Policy

Things you must not do

- Allow the use of Council Phones by unauthorised person(s)
- Use Council phones for personal calls (this includes the use of SMS text messages/internet use) except in an emergency
- Excessively use personal mobile phones during working hours to make calls, access the internet or send text messages
- Incur international roaming costs unless pre-authorised by your manager (or Democratic Services Manager, for members)
- Use phones in a manner that could bring Sefton Council into disrepute
- Send SMS or MMS messages that could contain discriminatory, abusive, racist, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content
- Send personal and/or sensitive data using SMS or MMS messages without verifying that the Council has the legal powers or explicit consent to do so.
- Use a Sefton Council number to promote any external private business
- Use a Sefton phone to contact premium rate numbers
- Remove the Council SIM card for any purpose (unless explicitly told to do so by a member of the ICT Service Desk as part of fault diagnosis/repair)
- Transfer the SIM Card to any personal device

If you receive any harassment via telephone, do not attempt to contact a person who has left you an unpleasant, suspicious or threatening message. Do not engage in conversation with a person making an unwanted call. Remain calm and try not to show emotion. Put the handset to one side for a few minutes then replace it. Record the date and time of the call as well as the details even if they were unanswered or silent calls. Write down and save any text messages and the time they were received. In the first instance users should inform their line manager and contact HR for further advice.

7. Security

All computer equipment should be placed in suitable physical locations that

- Reduce risk from environmental hazards, for example; heat, fire, smoke, water, dust and vibration
- Reduce the risk of theft
- Facilitates workstations handling personal data being positioned so that the screen cannot be seen by unauthorised personnel
- All items of equipment must be maintained on a departmental inventory
- When working in an agile way users are responsible for the security of device(s), some key general guidance notes are provided below

    - Ensure the device is logged out of the network when not in use
    - Devices must not be left unattended in a public location
    - Conceal when transporting on leaving ie: in a parked car
    - Do not leave devices in parked cars overnight, even if they are concealed
    - Place in a safe place if the device is to be stored at home/away from the office

Reporting Information Security Events and Weaknesses

Security events, for example a Data Security Breach or a virus infection could quickly spread and cause data loss across the organisation. All users must be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users must:

- Note the symptoms and any error messages on screen
- Disconnect the workstation from the network if an infection is suspected (with assistance from IT Support Staff)

All security events should be reported immediately to the ICT Service Desk on ext 4999.

Appendix A - Starters Movers and Leavers

This document defines Sefton Council Policy for starters, movers and leavers across the Sefton Council IT estate. The integrity and performance of the IT environment is maintained by keeping the underlying IT environments tidy. The principal drivers for an effective Starters, Movers and Leavers policy and process are:

- Security – ensuring the Council network and information resources can only be accessed by authorised persons
- Cost- utility consumption-based pricing of IT services means costs are controlled by timely removal of leavers and if a mover has reduced IT service needs they can be amended
- Asset management – accurate knowledge of asset location and status is essential for maximising the utilisation of those resources and ensures IT support knows what assets an end user has and where they are normally located. The process also means assets can be recovered and redeployed as efficiently as possible.

Starters, Movers and Leavers Key Principles

- Managers are responsible for ordering any new ICT Kit required via the ICT Client team in advance of commencement. It is suggested that such requests should be made at the same time appointment is confirmed to ensure enough time for equipment to be ordered and built.

- Managers are responsible for ensuring that user accounts and associated permissions are requested for new staff at least 48 hours before they are due to commence employment

- Managers are responsible for ensuring that notification of leavers is provided to the ICT Service Desk as part of the exit process

- Movers Managers are responsible for notifying the service desk of any moves across departments/teams within Sefton and the removal of access to data/applications no longer relevant to a user's role, note all Sefton Council staff permanently moving between departments will be treated as a new starter, except for email creation

- All Sefton Council IT Accounts not accessed for longer than **30** days will be disabled

- All Sefton Council IT Accounts not accessed for longer than **90 days** will be deleted except for long term sickness or maternity that must be informed by a user's manager or direct instruction from HR

    - Note the data of leavers will be deleted along with the Account, this includes Emails and any documents saved in the users OneDrive. It is the managers responsibility to ensure any files relevant to a project or service should be

moved and saved to the relevant folder. A notice will be provided to the leaver's manager to confirm that data can be deleted.

- Work experience and contractors will only be created based upon standard departmental profiles

- All temporary staff require an expiration date on their account, their account will be disabled on that date unless informed by a user's manager or instructed otherwise from HR

- Cloning of Sefton Council IT User accounts is strictly forbidden

Appendix B – Data Retention (IT Systems)

This document does not replace the authorities Retention Schedule but outlines the core principles of how data will be managed on the IT Infrastructure, this document only relates to electronic files, paper files are not included in this policy.

- User data for confirmed leavers is to be deleted after 90 days this includes data and information stored in **OneDrive** and **Email**

- Managers are responsible for ensuring the removal of electronic information from systems once retention periods are expired.

- It is expected that business information required for regulatory purposes will be stored in the relevant business document management systems. For example, finance data must be stored in Oracle or finance server not in user's email.

- Where an end user device is a desktop the saving of information will be restricted, where the device is mobile then that device will have approved encryption methods enabled and are not to be circumvented. Usage of approved and encrypted devices for storage of information while conducting daily work activities is permitted. Such devices include Council tablets and other smart devices; however, users must upload content to the appropriate systems (e.g. planning photographs) and remove it from the device.

- Unauthorised use of any cloud storage or online file transfer sites e.g. drop box or We Transfer is prohibited by the policy and using any cloud storage not authorised may result in disciplinary action.