ISLINGTON

Islington Acceptable Use Policy

A council-wide information technology policy

Version 5

April 2019

Revision History

The following versions of this document have been created and released:

Date	Version	Reason for change	Author
01/03/2019	5.1	Annual review and update	David Wilde
18/03/2019	5.1	Corporate Governance Group Approval	David Wilde
02/04/2019	5.1	Corporate Management Board Approval	David Wilde
25/04/2019	5.1	Union consultation and approval	David Wilde

1 Introduction

The digital age brings with it advantages as well as threats. If used correctly, computer and telephony services can provide local authorities with the ability to serve our residents, customers and partners efficiently in an economical, secure, accessible and legally compliant manner.

1.1 Purpose

This policy sets out the mandatory measures and requirements applicable to the use of the Council's IT Systems. It should be read in conjunction with Council policies, procedures and guidance covering:

- Information Governance and records management, including General Data Protection Regulation (GDPR)
- Remote and flexible working
- Freedom of information
- Social media
- Staff conduct

1.2 Intended Audience

This policy applies to all members, established employees, temporary employees, agency staff, authorised third party employees and consultants/contractors who are provided with access to any council provided IT service not designated as a public facility. For the purpose of this policy, these people will be termed "users". Managers are responsible for ensuring all users under their control are aware of, understand and adhere to this policy.

1.3 Scope

The Council provides IT resources to its users for business use. Personal use of IT resources is permitted within the constraints defined in this document. Use of the Councils IT resources to operate a personally owned business or for personal financial gain is unacceptable.

All access to council IT systems is based upon business need and related to the post held and role undertaken. Managers should satisfy themselves as to the suitability of candidates' IT skills during the recruitment process and ensure IT training and skills needs analysis form part of ongoing staff management.

To ensure the effective operation of this policy and to safeguard the Council's interests, the Council reserves the right to use automated tools and selected manual intervention, where appropriate and necessary, to monitor usage of business IT systems and services in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

All IT devices issued by the Council are for business use with only incidental and reasonable personal use.

1.4 Non-Compliance

Non-Compliance with this framework and/or abuse of any electronic information, IT resources or breach of any of the IT Acceptable Use Policy clauses, may include disciplinary action up to and including termination of employment for staff. Sanctions imposed by the Council do not preclude possible criminal prosecution under relevant legislation.

This means the Council reserves the right to monitor your ICT activity/data on work devices and systems. The resulting information may be used to support disciplinary and other actions where the activity is inappropriate.

2 Mobile Devices, Email and Telephony

The Council may provide users with a variety of voice and data services and mobile devices such as desktop phones, mobile phones, tablet devices, smart phones and voice mail.

Policy	Users must:	Users must not:

Council Mobile device use	a) Install and activate the Council's mobile device management software on all council devices b) Avoid using a mobile device to discuss or view sensitive information in public places where possible c) Ensure incidental personal communications do not incur any cost to the council	a) Leave messages containing sensitive information on voice mail b) Use it to "screen" incoming calls or to avoid answering calls unless there is a genuine need c) Use the Wi-Fi Hotspot facility of any council mobile phone to connect non-council devices to the internet d) Use only a reasonable amount of mobile data – being for council business and minimal incidental personal use. In particular, do not download non-council video.
Identifying callers		Divulge sensitive information of a business or personal nature, unless they are: a) Sure of the other person's identity b) Confident they cannot be overheard by people with whom the information should not be shared
Council business on personal devices	Install and activate the Council's mobile device management software on personal devices that access council email and other corporate applications (e.g. InTune for mobiles and Citrix or other access portals).	a) Divert your work phone to your personal phone unless necessary to support flexible working or for operational needs b) As far as practicable, avoid allowing calls to go to voice mail. c) **Never** divert/forward emails from your council email account to your personal email account.
Internet Access	a) Access and use the Internet during working time for the purposes of council business b) Report any offensive or illegal content to the IT Help Me	Breach the council's Code of Conduct for staff when using the Internet
Email and other digital communications	a) Use the delegation functionality in email to grant or rescind access to delegates b) Use "Private" calendar appointments where the subject or content of a meeting should remain confidential c) Treat emails as permanent written records which may be read by persons other than the addressee d) Review their email mailbox regularly and delete messages that are no longer required e) Treat unsolicited emails from unknown sources with suspicion f) Retain relevant emails and attachments in an appropriate case	a) Send outbound email from generic email accounts set up to receive incoming email only b) Forward "chain" or "joke" emails to others c) Use non secure email where use of secure email is appropriate d) Seek to gain access to another users' mailbox without either their consent or the written approval of an Assistant Director or equivalent e) Use personal email for business use or as a means of accessing systems as a council employee f) Use council email for personal use

3 Security of Systems & Information

Policy	Users must:	Users must not:

Passwords	a) Keep their passwords secret b) Change them at least every 90 days c) Change passwords whenever prompted by the system to do so d) Use a mixture of upper and lower case letters, numbers and special characters e) Ensure passwords are a minimum of 8 characters in length	a) Write down their passwords b) Allow anyone else to use a computer through their account (Login) c) attempt to access a computer system for which they have no authorised access d) use obvious words or phrases as passwords e) share their password with any other person. This also includes NOT sharing their password with another employee as a means of providing delegate access
Personal Identification Numbers (PIN)	change from default pin numbers to something different and unobvious	a) comprise simple ascending or descending sequences b) Be made up of the same digits
Screens and devices	a) Position screens and/or use a privacy filter so they are not overlooked by unauthorised persons b) Be locked at all times when left unattended (⊞ + L) c) Ensure all screens, PCs and laptops are logged off and closed down when not in use	a) be left unlocked and logged on when not in use
Data Storage	a) Store files and other data/media on council provided encrypted file stores b) Hold information at a level of security appropriate to its classification c) Use OneDrive to store information to which access has to be restricted to their personal logon ID	a) store data on local drives or removable media, as these are not backed up b) store data on an unencrypted device or unencrypted removable media c) store data in third party environments outside the control/management of the Council d) attempt to use personally owned removable media

4 Password Exceptions

In emergency circumstances, access to an individual's account may be granted to their line manager, Internal Audit or other appropriate party (via password reset or other methods). The following controls shall apply:

A. The request must be made via ICT Help Me and contain authorisation by an Assistant Director or Chief Officer giving a clear business justification for the access

B. The party gaining access to the account must abide by all relevant legislation, policies and guidance and only use the access for the specific purpose given in their justification

5 Equipment & Software

Policy	**Users must:**	**Users must not:**
Computer software	a) Only use council approved and supplied software with council IT systems and devices b) Submit any requests for new software products and services via the ICT help me	a) Attempt to purchase, download or install any software themselves on council IT b) Purchase any software or related IT cloud services without written authority from Digital Services

Computer Hardware	a) Only connect council provided and approved hardware to the IT network b) Procure all new hardware via ICT help me c) Secure written IT service desk approval to connect any third party device to the IT network	a) Attempt to purchase or install hardware themselves, irrespective of how it is intended to be used b) Connect any personally owned equipment to Council equipment, including USB ports and network ports c) Attempt to access services on the restricted government networks from a personally owned device
Cyber security	a) Report all potential and actual cyber security incidents as an incident on ICT help me b) Follow any instructions given by Digital Services regarding cyber security threats or breaches	a) Attempt to disable any of the cyber security measures in place b) Attempt to open or upload any links, files or other attachments from an untrusted source c) continue to use a device that may be compromised
Working flexibly	a) Ensure they sign for any council provided equipment b) Ensure they have appropriate authorisations for access to data off site c) Report all losses or theft of equipment to your line manager and the IT service desk. Where equipment was stolen or lost off site, also report the incident to the Police	a) Leave any equipment unattended when off-site b) Leave devices logged on or unlocked when not in use c) Allow unauthorised users to access equipment, systems or data
Remote access	a) If access to the council's network is required abroad, you must make a request via ICT help me together with your Senior Manager's approval b) Ensure systems and displays are not easily visible to others, especially in public places c) Avoid storing/carrying the two devices used for 2 factor authentication together	a) Use personal equipment to access council systems or data except via a council approved and issued secure connection b) Allow unauthorised people to access, connect to or use Council provided access
Termination of employment	a) Return all equipment and data (including files) to the Council in good condition b) If you are a Managers, then follow the HR leavers process; complete the leavers checklist; and ensure all IT assets are returned to Digital Services	a) Copy or remove data or other physical or digital assets over which the council has some responsibility