THE LONDON BOROUGH
www.bromley.gov.uk

Policy Document

Acceptable Use Policy for ICT

October 2021

THIS DOCUMENT REQUIRES DIGITALLY ACCEPTANCE VIA THE COUNCIL'S ONLINE TRAINING AND GOVERNANCE SUITE. A RECORD OF YOUR ACCEPTANCE WILL BE KEPT IN LINE WITH HR RETENTION POLICIES

Organisation	London Borough of Bromley
Title	Acceptable Use Policy for ICT
Author	Lucinda Bowen
File Name	Acceptable Use Policy for ICT
Owner	Lucinda Bowen
Subject	Information Governance
Protective marking	Not Protected
Review Date	23/09/2019

Revision History

Revision Date	Reviser	Version	Description of Revision
22/11/2019	Lucinda Bowen	1.0	Approved version
27/11/2020	Matthew Smallwood-Conway	1.1	Minor updates
14/10/2021	Lucinda Bowen	1.2	Updating links, terminology and mobile apps

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
IG Sub-group		
DPO	Mark Bowen	

Document Distribution

This document will be distributed to:
All officers and staff

Contents

THIS DOCUMENT REQUIRES DIGITALLY ACCEPTANCE VIA THE COUNCIL'S ONLINE TRAINING AND GOVERNANCE SUITE.

BY DIGITALLY ACCEPTING THIS DOCUMENT YOU ARE AGREEING TO ABIDE BY THE TERMS SET OUT IN THE POLICY.

A RECORD OF YOUR ACCEPTANCE WILL BE KEPT IN LINE WITH HR RETENTION POLICIES.

1. Introduction

Bromley Council values the capabilities of ICT systems and facilities it offers to authorised users. The use of ICT can bring significant benefits to Council activities and the delivery of its services but it can also introduce substantial risks to its operations. The Council aims to provide a safe framework and ensure the use of its ICT complies with current legislation.

This document represents the Council's policy on how these facilities should be used in the context of both work and personal use.

1.1 Governance

In line with the requirements of ISO27001, the recognised international standard for information security management, this policy will be reviewed no less often than once per year.

The Council's Head of Information Management (or equivalent) has responsibility for ensuring the annual review and that any proposed changes comply with current standards for best practice.

Any proposed changes or rationale for ratifying an un-changed policy must be approved by the Information Governance Sub-group and the Data Protection Officer.

1.2 Scope

This policy applies to all officers including, but not limited to, employees, contractors, agency workers, consultants and partners who have been permitted access by the Council to use or access LBB data on its behalf. It further includes Bromley Councillors when acting on behalf of the Council.

1.3 Purpose

This policy sets out some basic rules for making the best use of the Council's ICT systems and contains details of what is and what is not acceptable use. It

will help all ICT users know what standards are expected, how to follow this policy and explains what can happen if staff misuse the facilities.

1.4 Responsibilities

The Council's Data Protection Officer has overall responsibility for ensuring the effective implementation of this policy. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to the Council's operations lies with the Head of Information Management

All managers have a specific responsibility to ensure that their processes and procedures are carried out within the boundaries of this policy, that all employees understand the standards of behaviour expected of them and to take action when behaviour falls below its requirements.

All employees are required to make themselves aware of the Council's Information Security policies found on the Information Management page of Transform. More specifically this policy should be read in conjunction with the Data Protection Policy, Network Security Policy and Account Password Policy.

2. Private/Personal use of ICT systems, services and facilities

The Council permits your personal use of its ICT systems in your own time provided it does not interfere with your work and that your use is in accordance with this policy and subject to the conditions set out above. Personal use is a privilege and not a right. It must be neither abused nor overused and the Council reserves the right to withdraw its permission at any time.

Use for or in connection for private business purposes or any employment other than employment with the council is expressly prohibited.

Employees are advised not to conduct online payments. This is due to the information potentially being stored in cookies locally on your computer, which potentially could be compromised with the risk that it could be compromised by malware. If employees use the Internet to buy goods or services, the Council will not accept liability for default of payment or for security of any personal information provided.

The Council is also not liable for any personal injury (save where they council is negligent), financial loss, or hurt arising from the misuse of its ICT systems.

3. General Standards

2.1 Email

All employees are required to handle personal information in accordance with data protection laws. Further information about handling personal data is available in the Council's Data Protection Policy.

All communications via email should be professional and business like. Emails may be covered by the Freedom of Information (FOI) Act, Data Protection Act, Right of Access and Environmental Information Regulations (EIR). This means that they could be disclosed as part of an FOI request for information, a Subject Access Request or as part of any legal proceedings. Staff should always exercise the same caution on email content as they would in more formal correspondence.

When replying and forwarding emails, consider the content in the email trail further down in the body of the message.

Ensure that any sensitive or personal information that has previously been discussed is either removed, redacted or that you are within the law to disclose to the next recipient(s). Consider removing any such information before including original emails in attachments or as part of the conversation history from a long chain of email correspondence.

If you receive an email that you believe to be illegitimate please send it to infosecurity@bromley.gov.uk as an attachment, do not reply to the email, click any links or open attachments. If you have replied, clicked any of the links or opened the attachments then contact the IT Service Desk.

If information by way of an attachment or comments in the email trail is disclosed to unauthorised recipients a data breach has occurred and may need to be reported to the Information Commissioner's Officer (ICO). The consequences of the report notification could be loss of reputation and/or a fine for the organisation and disciplinary and/or legal proceedings to the individual who caused the breach.
Auto-forwarding emails is not permitted. This is because email that is automatically forwarded by-passes all the measures the Council has put in place to check the content and origin of these emails. This would mean that sensitive, RESTRICTED data could be sent automatically to email accounts that are not sufficiently secure.

For more information about keeping data safe please see the Council's Data Protection and Confidentiality Policy

Your Bromley.gov.uk e-mail address must only be used when acting as an employee of the Council, and should not be used as a point of contact in a personal capacity.

The Council may have cause to access mailboxes for legitimate business purposes, without express permission, including but not limited to when an employee is absent or after staff have left the Council. Such access will be approved by the Director of HR & Customer Services in liaison with the Director of Corporate Services.

2.2 Internet

The Council's internet service is protected by filtering software, which prevents access to internet content deemed unacceptable in the workplace or that is likely to increase the risk of malware entering the corporate network.

From time to time you may inadvertently access a site that should not be available but has somehow evaded the filtering software. If you open a web page that you believe should be blocked due to inappropriate content, simply send the address details of the page to the IT Service Desk so appropriate action can be taken to block access to the site.

Blocked sites may be made available to individual internet users or group of users where there are sound business reasons for doing so, and following a risk assessment and approval by the appropriate line manager. To apply for access to a blocked site contact the ISD team.

2.3 Skype

Skype for Business is the Council's telephony service and allows for voice, video and instant messaging communications. Skype also allows for the sharing of desktops screens for training, troubleshooting and efficient working. Consideration needs to be given to the desktop background and other visible information so as to prevent inadvertent disclosure.

Skype must only be used for business collaboration purposes. Communication using Skype for Business should be conducted in the same manner as emails and fall within the guidelines at paragraph 2.1

Calls for personal use are not permitted unless authorised by your line manager.

2.4 Messenger

Where possible staff should use messenger for more informal discussion of work related matters where an email is not required. Messages sent using Instant messenger will only be retained for a limited period before being deleted. For more formal correspondence or where messages need to be retained for a longer period of time email should be used.

Logs from messenger may be accessed by the Council in the same way as email.

2.5 Document Storage

All electronic work documents and files should be stored in the correct repository depending on departmental processes and procedures and cleansed either automatically or manually in line with the corporate retention schedule.

Material received created or stored in a work or employment capacity is owned by the council and must be manged by the user in accordance with the Council`s document retention and destruction polices and may only be deleted in under such policy.
The Council may have cause to access document repositories for legitimate business purposes, without express permission, including but not limited to when an employee is absent or after staff have left the Council Such access will be approved by the Director of HR & Customer Services in liaison with the Director of Corporate Services.

The following repositories are available:

a) OneDrive - personal storage location provided as a replacement for the M: drive.
   OneDrive serves as a repository primarily for an officer's own HR related information, confidential information and draft documents not ready for dissemination.
   It is the officer's responsibility to ensure that information held in OneDrive is manually deleted in line with the Council's retention schedule;

b) Shared Drive – this area is for general storage of operational files and the use is directed by relevant business processes.
   The logical structure will be determined by the functions within each department;

c) SharePoint - an Electronic Document and Records Management System (EDRMS) for storing and sharing business information and as an intranet communication and knowledge base environment.

The implementation of retention policies, metadata (definition) and classification helps to ensure that the Council remains compliant with its data protection obligations and that an appropriate level of security is attributed to the stored information.

Adherence to these policies, permissions and general good practice use of the systems is essential to maintain the confidentiality, integrity and availability of Council information.

2.6 Bromley managed machines

All ICT equipment provided to users remains the property of the Council. It is to be returned to the IT department if it becomes defective or when no longer required for the role in which it was issued, for example, at the end of term in elected office, end of employment or end of contract.

All authorised users are accountable for all screen activity and transactions entered through their User ID whether or not they were present at the time. When IT equipment is left unattended officers should ensure that they 'lock' their computer screen to protect their work and access to any sensitive information they may have access to.

2.7 Non-Bromley managed machines

Whenever using public machines (i.e. from libraries, cafes) officers should ensure that they always 'lock' their computer screen to protect their work and access to any sensitive information they may have access to.

When working from home officers should note that local hard-disks are not suitable locations to store important work-related information as the disks are not backed-up and so data will be lost if the machine fails or is re-built by ICT.

Accessing and storing Council cloud hosted information via downloaded apps on personal PC's, mobile devices and smart technology is in breach of the Council's data protection policies.

2.8 Mobile phones

Mobile telephones will only be available to staff who have the approval of their line manager and authorisation of the appropriate Head of Service. An employee will be eligible to have a mobile phone if it is deemed necessary to their position, and they meet any one of the following criteria:

- If the employee's duties require them to spend a substantial amount of time out of the office on work related duties;
- Staff for whom it is necessary to make essential work-related calls off site, as part of their normal course of work;
- Staff who are required to be contactable in an emergency situation, when working off-site;
- Staff who are on call after normal business hours;
- Staff identified through the risk assessment procedure;

Once a mobile device has been assigned the following conditions will apply to its use:

- Anyone wishing to install any personal App on a Council provided mobile device must consult IT before doing so;

- Excessive personal use of a Council-provided mobile device may be regarded as misuse and treated as a disciplinary matter.

2.9 Social media and messaging service i.e. WhatsApp, YouTube

The Council actively uses social media to promote its corporate events and to connect with customers. A set of standards has been established to ensure consistency and effectiveness and any business unit who wishes to use social media should consult with the Public Affairs team.

All corporate use of social media, where permitted, must be in line with the Council's communication strategy and it is the responsibility of local managers to ensure careful monitoring and best practice.

Please note that people will have a different level of comfort with social media. Ensure a different means of communication is provided where individuals do not wish to engage via a social media platform.

All communications sent or received via social media, regardless of format (text, chat, WhatsApp, YouTube videos etc.) should for practical purposes be considered to be on the public domain. They are therefore subject to the same legislation as any other Council publications including the Data Protection Act, Freedom of Information Act etc.

Staff should not:

- Accept or initiate contact with a current or former client of the Council or their family via a social networking site;

- Make available any personal or sensitive personal information belonging to a current or former client of the Council or their family via a social networking site;

- Make available any images (including videos) of any current or former client of the Council via a social networking site.

4. Remote access

The network can be accessed from a home or public Wi-Fi connection via remote access. The use of the Council's facilities from a remote location is classed as business communication and may be monitored and/or required as legal records.

Users should never leave any Council's mobile ICT equipment unsecured or unattended and always take precautions to avoid unauthorised access.

5. Monitoring

The Council is ultimately responsible and accountable for all business communications transmitted by and stored on its information and communications systems.

Because of the need to protect its network, it may be necessary to scan or monitor information stored on any computer, tablet or networked device belonging to the Council to ensure that:

- Staff do not bring the Council into disrepute by abusing the service;
- Internet access to sites is within legal boundaries;
- It is not inadvertently providing staff with a means of breaking the law;
- The Council itself is not breaking the law through the actions of its staff;
- Many malicious attacks by viruses and other malware - programs designed to cause harm to IT systems - can be inadvertently accessed via the internet. It is important to stop these infecting the network, and to track down the source of a virus and the route that a particular program has used to infiltrate the network if it does get through. Usage logs can be used to help find this information.

6. Software

Users must not install any software on Council machines unless authorised to do so by ISD. Any requirement for software should be requested through the IT service desk.

Council software must not be installed and/or downloaded onto non-Council devices.

Please remember not to block software services like anti-virus and malware and allow updates to run and restart machines in a timely manner.

7. Removable media / cloud storage

No Council data should be copied to removable media without express authorisation of the line manager. Where authorised, removable media should be encrypted, virus checked and stored securely.

It is important to check the source of the removable media and never pick up a device and plug it into the corporate network if found lying around.

You should not copy any Council data on to your personal cloud storage systems such as Dropbox, Google Drive etc. as they are unlikely to provide the same level of security.

8. Unacceptable use of ICT systems

Unacceptable usage includes but is not limited to:

- excessive use of email or the internet to the detriment of the business and the user's performance;
- using the internet for personal reasons during core business hours;
- printing of large documents and wasteful use of resources;
- sending and/or storing large quantities of material that are not job related;
- transmitting lewd material, jokes, joke programs, games etc;
- sending and/or storing abusive or offensive material;
- taking part in chain or pyramid letters or similar schemes;
- using foul or abusive language;
- carrying out private work, paid or unpaid;
- using the internet or e-mail to harass or harm others;
- intentionally accessing, sending or creating computer viruses or other malicious software designed to damage information systems or steal information;
- attempting to disable, damage or otherwise impede anti-virus or other security systems on any Council equipment;
- trying to find ways of bypassing or getting around the safeguards put in place to protect access or prevent the monitoring of the user's usage;
- using someone else's account;
- allowing others such as family or friends to use systems or equipment provided by the Council;
- on-line gambling or gaming;
- potentially bringing the Council into disrepute through inappropriate actions;
- knowingly doing anything illegal under English law or the law of any other relevant country.

Except as agreed with management as part of documented and monitored business process, staff should not:

- Make available any personal or sensitive personal information concerning an employee of the Council in relation to their employment, including judgements on their performance and character;
- Make available any images of an employee of the Council in their work situation;
- Express any views or take part in conversations, either positive or negative concerning the functions of the Council or the performance of any of its employees;
- Express any views that might be taken to represent the official view of the Council without first consulting the Communications' team.

9. Acceptable use policy for ICT sign-off

This Policy contains important information which is relevant to all employees. It is your responsibility to be familiar with the contents and comply with the policy. Once you have read and understood this Policy, please digitally accept the policy.

Bromley Council provides equipment and systems to help colleagues with their work. This policy provides clear rules designed to protect the Council, its staff and customers.

BY DIGITALLY ACCEPTING THIS DOCUMENT YOU ARE:

- Agreeing to comply with the terms of this policy governing the access to Bromley Council's systems and data. I understand that any breach of this policy could lead to disciplinary proceedings being taken against me in accordance with Council policies and procedures.

- Understand that all equipment provided remains the property of London Borough of Bromley.

- Confirm that I will return all equipment along with my security pass on my last day of service.