BARNET
LONDON BOROUGH

Acceptable Use Policy

London Borough of Barnet

Document Control

Document Description	Acceptable Use Policy		
Version	8		
Date Created	January 2009		
Status	Final		
Document Owner	XXXXXXXX, Information Security Manager, Information Systems, XXXXXX@barnet.gov.uk, 020 8359 7117		
Document Classification:	Not protectively marked		
Authorisation	Name	Signature	Date
Prepared By:			
Checked By			

Version Control

Version number	Date	Author	Reason for New Version
1	Jan 2009	XXXXXX	New Policy
2	Sep 2010	XXXXXX	Formatting revision
3	27/07/11	XXXXXX	Style updates and initial review by IMWG
4	31/08/11	XXXXXX	Content update for IMWG Policy Map
5	29/09/11	XXXXXX	Structure changes prior to IMWG review
6	16/11/11	XXXXXX	Addition of clause on personal data
6.1	27/06/12	XXXXXX	Changes from Corporate Governance, CAFT, Legal incorporated.
6.2	23/08/12	XXXXXX	Update to use of personal email
7	17/10/12	XXXXXX	Section 5 updated to include systems access after IGC Action and feedback from IG Group, SIRT & CAFT incorporated
8	10/03/14	XXXXXXX	Full review. Personal use moved to own section. Ownership of equipment and Member use clarified. Business continuity included.

Contents

1. Introduction

The purpose of this policy is to:

- protect the information assets owned and used by the council;
- protect other services or networks to which the council is connected from misuse;
- ensure compliance with all regulatory, legislative and internal policy requirements.

This policy applies to users of computer services and equipment that are provided by London Borough of Barnet (LBB), or its ICT providers; including Members, employees, temporary staff, contractors, partners and any authorised 3rd parties. It does not apply to council services provided to the public. It also applies to the use of services on all council devices including mobile equipment such as BlackBerrys or mobile phones and tablets or laptops. Please note this policy applies:

- whether you are using the equipment at work or off council property.
- when using the equipment with any internet connection whether work, personal or public.

Any actual or suspected breaches of this policy will be thoroughly investigated, and in the event of staff or Member misconduct will be dealt with under the council's disciplinary procedure or the Member's Code of Conduct complaints procedure respectively. Any suspected breaches that may constitute a criminal offence will also be reported to the council's Corporate Anti Fraud Team (CAFT) for investigation.

Staff are responsible for identifying to their line manager any concerns with work processes or other local arrangements that prevent them from complying with this policy. Line managers are responsible for ensuring that staff are supported in complying with this policy. Members should seek advice from the Council's Chief Finance Officer or Monitoring Officer when using resources of the Council if there are concerns regarding complying with this policy.

Access to council information systems and equipment is provided by the council for Members to use in their three roles of Member of the Council, ward representative and political party/independent member. The equipment belongs to the council throughout its useful life. At the end of its useful life the council may consider options for Members purchasing the equipment, however this should not be assumed.

It is recognised that Members will use equipment and systems outside of traditional working hours and mainly from private or public internet connections. However, the

principles in this policy apply to all Members as they do to staff, with the exception that Members can use council email for communication of political beliefs.

Suspected breaches of this policy by Members may warrant investigation and in any event will be reported to the Leader of the Council, Leader of the relevant Party Group, Chief Executive and/ or Monitoring Officer. Any suspected breaches that may constitute a criminal offence will also be reported to the council's Corporate Anti-Fraud Team (CAFT) for investigation.

2. General Computer Use

2.1 Passwords

Access to Council systems and data is through user identification and passwords. Mobile phone must be protected with a PIN number; BlackBerrys with a 'strong' password as described in the BlackBerry User Policy. The characteristics of a 'strong' password include the following:

- At least 8 characters long
- A mix of alphabetic, numeric and special characters
- Not based on a pattern e.g. 12345678

Further information is included within the Password Policy.

2.2 Personal use

Access to council information systems and equipment is provided to assist users in the performance of their jobs. Where access and equipment is provided its use should be limited to official council business. However, it is recognised that there may be occasions outside of work time or during lunch breaks when users wish to use them for personal reasons. Reasonable personal use of council internet and email services is permitted provided it complies with this policy and any policies and legislation referred to in this policy.

Examples of unreasonable personal use are:

- The use of council Information Communication Technology (ICT) services to operate any business or for work outside of council employment.
- When the personal use of internet facilities affects a user's work performance.
- Time wasting and large amounts of continuous usage.
- Wasteful use of resources.

- Saving of non-council data on the council network (including 'home drives'). These can and will be deleted to minimise expenditure on storage and back-ups.
- The printing of large documents.
- Sending or receiving large documents or large numbers of emails.
- Access to websites prohibited under council policies (including material considered offensive in any way such as sexually explicit, discriminatory, defamatory or libellous material).
- The use of systems or the internet for personal gain, examples include gambling and trading. No personal websites may be hosted on council equipment.
- Use of the system should not have a noticeable effect on the availability of the system for others. Therefore users should not participate in resource intensive online games or have active any web channels that broadcast frequent updates to your computer.

Under no circumstances should users allow others such as family or friends to use systems or equipment provided by the council.

All users of council systems are responsible for the professional, ethical and lawful use of those systems. Access is granted on the basis that the user understands and adheres to this policy and agrees that system usage, including personal use, will be subject to monitoring by the council for policy compliance.

2.3 Hardware use

All ICT equipment provided to users including Members, employees, temporary staff, contractors, partners and any authorised 3rd parties remains the property of the council. It is to be returned to LBB 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.

No council data should be copied to removable media without express authorisation.

No peripheral devices of any kind (cameras, PDAs, mobile phones, unencrypted USB drives etc) may be installed or configured on, or connected to any council computer unless authorised and installed by Information Services (IS). If you have a requirement to use the CD drive or USB ports on any equipment you will need to raise a policy exception request by contacting the IT service desk.

2.4 Remote working

Only corporately managed machines (computers and mobile equipment such as phones and tablet devices) may be used to access the LBB network and its systems

and / or to work on Council information. The network can be accessed from a home broadband or public wifi via Citrix or VPN, or through Mobile Iron technology on tablet devices.

More detailed information (for staff) is included in the Remote Working Policy.

2.5 Use of personal equipment or email accounts

On a day to day basis the use of personally owned equipment or personal email accounts for council business is forbidden. If working from home is required on either a regular or ad hoc basis this should only be conducted on council or authorised 3rd party equipment.

However, during business continuity incidents such as building failures or extreme weather it is accepted that some council business could be conducted on personal equipment when agreed by your line manager. Personal information must only be dealt with when absolutely necessary and not for the sake of convenience. Sensitive personal data (as defined by the Data Protection Act 1998, such as medical or equalities information) should never be sent to or processed using non-council provided equipment.

Any use of personal email accounts for business continuity purposes should copy in your work account to ensure that the council has an appropriate record of its business. Council data must be deleted from personal equipment and email accounts as soon as the necessity to use personal equipment is over.

It is expected that users will prepare for expected events such as tube strikes or forecast bad weather and take equipment home with the approval of their line manager if it is expected that attendance at work would not be possible.

2.6 Social media

The Council's Social Media Policy provides a framework for the effective, compliant and secure use of social media to promote and develop the council's objectives, services and achievements; providing information about council services to service users. It provides guidance to staff on best practice when using the medium in a professional capacity whilst protecting the reputation of the council and allowing the safe and controlled roll-out of social media across the organisation.

Specifically for Members, the council will support the use of social media by Members in their committee roles. It will provide advice on the establishment of an account by any Member of the Council. Council officers cannot support the use of any medium for party political matters. Committee Members should use 'Cllr' accounts for party political issues. Members should always keep clear distinctions between council business, political business and personal business. It is recommended that Members have separate accounts for different roles.

2.7 User responsibilities for the care of ICT equipment

You must immediately report any loss or disposal of council ICT equipment to your line manager, the Information Management team on x2029, Insurance on x7197 and the IT service desk on 020 8359 3333 during office hours.

2.8 Software installation

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

Council software must not be loaded onto non-council devices.

2.9 Fault reporting

All IT faults and IT security issues should be reported to the IT service desk.

The Service Desk is open between 8am and 6pm, Monday to Friday.

Telephone extension x3333 or email ITservicedesk@barnet.gov.uk.

3. Email Services

The email system is provided to assist users in the execution of their council duties. The email section of this policy applies to both internal and external emails.

3.1 Use of council email system

The use of email should be handled with care; consequently, users should be aware of the following:

- Email auto forwarding to external addresses is forbidden.
- No user must use the council's email system in any way that may be interpreted as insulting, threatening, abusive, disruptive or offensive by any person or company, or anything that may be harmful to council morale or reputation.
- Examples of prohibited material include:
    - Sexually explicit messages, images, cartoons or jokes; unsolicited propositions; profanity, obscenity, slander or libel; ethnic, religious, or racial slurs; political beliefs (acceptable for Members), lobbying or canvassing;
    - Any message that could be construed as harassment or disparagement of others. In particular, but not limited to those based on their sex, race, sexual orientation, age, national origin, disability, religious, or political beliefs.

    - Any message that incites or depicts violence, or describes techniques for criminal or terrorist acts.

- Email communications are not guaranteed to be private, arrive at their destination within a particular time, or at all. Emails are subject to the same laws as other forms of communication, and could render the user and council liable to actions for defamation.

- Email content may be subject to disclosure under the Freedom of Information Act 2000 and the Data Protection Act 1998.

- Users must not send unsolicited, irrelevant or inappropriate email to multiple newsgroups or to mailing lists on the internet.

- The forwarding of chain letters is forbidden. This includes those purporting to be for charity or other good causes. Virus warnings come under the same exclusion and should be discussed with the IT service desk, but should not be forwarded to anyone inside or outside the council.

- Users must not misrepresent themselves or use anonymous mailing services to conceal their identity when mailing through the internet, falsify emails to make them appear to originate from someone else, or provide false information to any internet service which requests name, email address or other details.

- The user logged in at a computer will be considered the author of any messages sent from that computer. Remember to log-out, or lock your computer when you leave your desk. Under no circumstances should you send an email from a device that you have not logged into.

- Attachments in email messages often contain viruses, and will likely appear to come from someone you know. Read the text part first. You can often judge by the language used whether it looks right for the sender. If you feel it is not genuine, do not attempt to open the attachment. Contact the IT service desk for assistance.

- Users should not access emails not intended for them, even if they are not protected by security controls, or do anything which would adversely affect the ability of others to access emails or internet resources that they are entitled to access.

- Be aware that council and 3rd party email systems can and do support proxy (delegate) access to email.

- If sending Sensitive Personal Data (as defined by the Data Protection Act 1998) electronically, a secure email system provided by the council should be used.

- Emails that are sent using GCSx services are required to be protectively marked in accordance with the council's Protective Marking for GCSx Emails Policy

3.2 Best practices for email usage

It is important to recognise that email folders are not a good mechanism for long-term retention of council data. Under the Data Protection Act, the council must not hold data for longer than it is needed. If it is necessary to retain information from an email it should be stored in a more accessible form; if it is not necessary to retain the information it should be deleted:

- All users of email are required to ensure that messages are deleted when the information they contain is no longer required (or has been saved appropriately elsewhere).
- All users of email are required to ensure that information in their mailbox is moved out to a more appropriate form of storage if it must be retained and used by others in the council (eg a document management or case management system). This is especially applicable to attachments or to emails that contain personal information relating to others.
- The use of Personal Folders is not recommended.

3.3 Data Protection and Email

Sensitive Personal Data (as defined by the Data Protection Act 1998) and highly confidential information when sent externally must only be sent via secure email such as GCSx or Encrypt and Send. Users are responsible for considering the sensitivity of data in an email before they send it and choosing the most appropriate method of transfer.

3.4 GCSx Email Accounts

GCSX email accounts should be used for the sending of sensitive personal data. An account can be requested from IS self-service. Users of GCSx email accounts should refer to the council's "Protective Marking for GCSx Emails Policy" before use. GCSx emails can only be sent to other users on the secure PSN network. Where communication is outside the scope of the GCSx system the council alternative secure mail systems should be used.

4. Internet Services

Access to the internet is provided to assist employees in the performance of their council duties. Where access is provided use should be limited to official council business or fall within the guidelines set out in section 2.2.

4.1 Use of council internet services

The use of the internet must be handled with care. Users should be aware of the following:

- In line with the Social Media Policy, staff should not post messages on any internet message boards or other similar web based service that would have an adverse effect on the council or which a reasonable person would consider to be offensive or abusive. The list of prohibited material is the same as those for email listed in 3.1.

- As part of routine security measures, all websites visited are centrally logged. The council monitors and logs all internet accesses by individuals and reserves the right to access and report on this information.

- You should not visit websites that display material of a pornographic nature, or which contain material that may be considered offensive. It is recognised that you may accidentally open a site which has such material, if this happens you should contact the IT service desk immediately.

- You should not enter your work email address on a website except on council business approved by your line manager.

- The person logged onto a computer will be considered to be the person browsing the internet. You must log out or lock your computer when leaving your desk to ensure that no unauthorised use of your computer can take place. Under no circumstances should you browse the internet, or use systems, from a computer that you have not logged into.

- You should not use unauthorised cloud storage such as DropBox, Google Docs and similar applications for council data without permission from IS or IMT.

4.2 Anti-virus

Users must not recklessly introduce a computer virus or malicious code into council computers. Deliberate introduction or transmission of any virus, or software designed for breaching security controls or creating computer viruses is an offence under the Computer Misuse Act 1990. A policy of virus checking on all executable code sent by electronic means is in place. Virus protection software is installed on all council computer equipment:

- No attempt should be made to bypass or disable the virus protection, or to turn off or delay the periodic updates.

- Any employee who suspects that his/her workstation or laptop has been infected by a virus or malicious code must immediately call the IT service

desk, disconnect the device from the council network and stop using the computer.

- All internet emails and their attachments received and sent by the council's network are virus checked and encrypted mail will be blocked if it cannot be virus checked.
- Do not follow unsolicited links including those received via email, web fora etc.
- Any employee recklessly transmitting a virus or malicious code to or from council computers is in breach of this policy.
- Incoming media shall be scanned for viruses before they are read. Employees shall only load media under approval from the IS department.

5. Systems Use

5.1 Systems Access

Line/Hiring managers should ensure that all new users have the correct access at the appropriate level to any systems they may require to effectively carry out their role. They must also ensure that users do not have access to any personal or sensitive data that is not required, as this would be breach of the Data Protection Act.

Information Services, in consultation with the Governance Team within the Assurance Group, will ensure that Members have the appropriate level of access to effectively carry out their role.

If a user changes role/service their systems access must be reviewed to ensure only appropriate levels of access are available. This is the line/hiring managers responsibility. Similarly, when a user leaves LBB their line/hiring manager is responsible for completing the leaver process/checklist including updating/ceasing this access. The line manager will be held accountable in the event of a data breach resulting from the failure to assure the correct level of access. In the case of Members, this responsibility falls to the Head of Governance.

All users have the responsibility to inform their manager immediately if they become aware that they have access to any records, drives or systems that they do not legitimately require to effectively carry out their role. In the case of Members they should inform the Head of Governance if they become aware that they have access to any records, drives or systems that they do not require to effectively carry out their role.

5.2 Monitoring of Systems Use

The council may, for authorised monitoring purposes, view any system transactions, read any email and attachment drafted, sent or received at work; or view any internet site visits or transactions, in particular to check policy compliance. However, every effort will be made to avoid unnecessary access to content which is clearly marked as 'personal', unless those emails form part of an investigation into the use of IT equipment.

Such monitoring and subsequent reports will be restricted to authorised persons. Usage reports measuring frequency and size of emails, sent or received, and the extent and frequency of internet use will be disclosed to authorised users undertaking investigations under this and other information policies. These reports may identify the user, destination or type of site.

System records may also be subject to access requests under Freedom of Information or Data Protection legislation.

Note, at the council's discretion of the Monitoring Officer such information may also be disclosed to specialist 3rd parties as part of LBB's own computer forensics investigations.

In addition, it may be necessary to access users' emails in order to prevent or detect crime, establish the existence of facts relevant to the council (e.g. gather evidence of a business transaction), to ascertain compliance with regulatory practices relevant to council business, disciplinary investigations / employment proceedings or checking for business relevant emails during absence.

If managers require access to a user's account for business purposes during a user's absence, this request should be made to the IT service desk.

If a technical problem arises with system content, for example a blocked mail item, it may also become necessary to send that content to a 3rd party for analysis/problem resolution.

6. Copyright Compliance

Information in electronic form may be subject to the Copyright, Designs and Patent Act 1988. This requires that you get permission from the owner of such information before making use of it in any way. The council has a CLA copyright license which permits employees (which includes temporary staff and contractors) to download, copy and reuse copyrighted material subject to license conditions. These can be found in the council's Copyright Policy.

The CLA license only covers council employees and therefore does not cover employees of CSG and Re, or Members. See the Council's Copyright Policy for more information.

Users should not copy information originated by others and re-post it without permission from, or at least acknowledgement of, the original source, even if the content is modified to some extent. Users should not assume that information posted on the internet actually originates from the person or organisation that appears to have produced it without some form of authentication.

Copyright and other rights in all messages posted on the internet from a council account, such as material produced at work, belongs to the council, and not to users personally.

If in doubt about copyright issues you should refer to the council's Copyright Policy.

7. Review of the Acceptable Use Policy

This policy will be reviewed on an annual basis or as required by policy or legislation changes.

8. Contact Information/Further Guidance

Further advice and guidance is available from the IS or the Information Management Team.

Address: London Borough of Barnet
Building 4
North London Business Park
Oakleigh Road South
London N11 1NP

Tel No: (020) 8359 3333
Email: ITServicedesk@barnet.gov.uk

Tel No : (020) 8359 2029
Emails : data.protection@barnet.gov.uk