Havering
LONDON BOROUGH

BUSINESS SYSTEMS POLICY

November 2010

Version 4.0

Table of Contents

Policy Governance:

Policy Review:

Role	Name
Senior Information Security Officer	Ian Lett
Human Resources	Various
Legal Services	Various
Trade Unions	Various
Internal Audit	Various

Policy Authorisation:

Role	Name
Head of Business Systems	Geoff Connell
Group Director of Finance & Commerce	Andrew Blake-Herbert

Document Version Control:

This Policy will be reviewed annually in the month of November unless a specific amendment is required that cannot wait until the next annual review.

Version.	Date	Description
0.10	14 Jan 2007	Draft version of policy for consultation
0.20	15 Feb 2007	Final Draft of policy for consultation
0.22	28 Feb 2007	Final Draft. For Approval
1.01	22 Sep 2007	First draft first review
1.02	01 Oct 2007	Final Draft for comment
1.9	22 Oct 2007	Final Draft. For Approval
2.0	01 April 2008	Final draft V2
2.1	01 May 2008	Minor Amendment v2.1
3.0	01 Aug 2008	Final draft for approval V3.0
4.0	26 Nov 2010	Final draft V4.0

1. Introduction:

1.1. The Key Points

The London Borough of Havering recognizes its dependence on information, communications and technology in delivering an effective service to the public. In order to protect these core assets this policy sets out the rules of what is and isn't acceptable when you are using all aspects of information, communications equipment and technology that the Council provides.

In order to build public confidence and ensure that the Council complies with relevant statutory legislation, it is vital that the Council maintains the highest standards of information security. As such, this policy is in place to maintain these high standards of information security.

If you don't have time at the moment to read the full Policy, please read the bullet points which are contained in boxes on each page. They explain what you must and must not do. When you have more time you can read the document in full for all the details.

The Policy also includes references to pages on the intranet where you can get more information. If you do not have access to the intranet contact the ICT Service Desk on ext.2515 and we will send you the documents you need.

All Managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff. It is important that every user of Council information is aware of their responsibility and understands the need for appropriate information security.

All users (e.g. Benefit Services) of the Government Connects Secure Extranet (GCSx) Secure Email who have access to "RESTRICTED" data must have completed the GCSx (Protecting Information) training course prior to having access to such data.

It is the responsibility of each member of staff and all users to adhere to the Policy.

Throughout the Policy instructions have been given to contact ICT Services regarding access restrictions. These are necessary to enable a primary aim of the Policy, that being to mitigate the following risks:-

- Unauthorised access to sensitive information, personal information, or documents marked as "PROTECT" or "RESTRICTED".
- Introduction of malicious software and viruses.

- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Reputational damage as a result of information loss or misuse.
- Increased risk of equipment damage, loss or theft.

1.2. Related Documents

Elected Members ICT Policy – TBA pending amendments
Data Protection Guidance
Information Classification Guidance – TBA pending amendments
GCSx Acceptable Usage Policy and Personal Commitment Statement
Disciplinary Procedure
Whistle Blowing Policy
Information Security Incident Reporting and Management Procedure

2. Objectives:

The objectives of this document are to:

- Ensure that the Council's information assets, voice and data communications equipment, and computer systems are protected.
- Ensure that users are aware of their obligations.
- Ensure that users are aware of the risks of non-compliance.
- Ensure that the Council has managed its risks where identifiable.
- Ensure that the Council complies with current Codes of Connection including:
  LPSN (London Public Service Network)
  GCSx (Government Connect Secure Network)
  N3 (NHS Secure National Network)
- Ensure that the Council complies with current legislation including:
- Human Rights Act 2000
  Data Protection Act 1998
  Local Government Act 2000
  Computer Misuse Act 1990
- Ensure that Members are aware of the Code and Protocol applying to the use of resources.

Procedures based on ISO 27001 (Formally ISO17799) exist to support the Policy. These include virus control, passwords and business continuity.

3. The Rules of This Policy:

3.1. World Wide Web

Access to the World Wide Web (The Internet) is primarily for business use. All use of the World Wide Web is monitored and logged.

Managers are responsible for monitoring Internet use within their own department or Service, for which management information can be provided by ICT services on request.

Any attempt to logon using another person's ID, or to try and circumvent the security systems may be regarded as a disciplinary matter.

Access to certain site such as, social networking, online chat and instant messaging and other non business sites are strictly controlled by the Information Security Officer and requests for access must be submitted to the ICT service desk and must have the line managers authorisation.

Many useful sites require registration and Users wishing to register on a website for work purposes are encouraged to do so. However, permission should be sought from an appropriate manager before doing so and if there is any doubt or concern the Information Security Officer should be consulted. Contact the ICT Service Desk for further information.

3.1.1. Business use:

Business use of the internet means using the internet in support of LBH policy's and business needs, specifically those needs that directly relate to your day to day duties.

You **MUST**:

- Be careful with business details including job title and email address when signing up for web-based business services.

You **MUST NOT**:

- Visit or view any web sites containing inappropriate material that is:
    - Sexual
    - Illegal
    - Homophobic
    - Racist
    - Religion intolerant
- Subscribe to any bulletin boards, news groups or any other Internet service of any kind unless it is part of normal day to day business operation.
- Use corporate credit cards online except on web sites sanctioned as safe to

use, contact Systems & Payments for full list.

- Download and/or install any software (games, applications screen savers) etc without authorisation from Business Systems.
- Download video and audio files without authorisation from Business Systems.
- Download and/or store any personal images.

3.1.2. Personal use:

Remember that the business use rules also apply to personal use of the internet. Any internet use (including the use of Webmail services) must be in your own personal time and must not exceed more than one hour a day. Similarly, this kind of use is acceptable for officers who operate Council equipment in their homes.

Personal use of the Internet must not contravene any specific management instructions or interfere with the performance of duties.

The council accepts no liability for loss or damage incurred as part of personal use of the internet.

You **MUST**:
• Be careful when using financial, banking and shopping sites. Use of such sites is at your personal risk.

You **MUST NOT**:
• Use the Internet (this includes the use of Webmail such as Hotmail, Gmail etc) for personal use in hours you are being paid to work i.e. Core and overtime hours.

3.1.3. Use of Social Networking/Blogging sites:

As with all other internet access the use of blogs and social networking sites will be monitored and logged.

Users may access personal blogs/social networking sites for their own use, provided that this is outside of working hours, and observes the restrictions outlined below.

Employees must also ensure they are compliant with any rules set out in the Council's Internet Policy and does not adversely impact on their council duties.

Users must not disclose any information that is confidential to the Council or any third party or disclose personal data or information about any individual/colleague/service user, which could be in breach of the Data Protection Act. Users must not post illegal material, e.g. images of child abuse or material which incites racial hatred, include any information, sourced from the Council, which breaches copyright, make defamatory remarks about the Council, colleagues or service users.

Additionally, users should not publish any material or comment that could undermine public confidence in the Council. Staff can have their own blogs etc and have the right to freedom of speech to express in their own time their own personal opinions provided it is not unlawful, defamatory, discriminatory or misrepresentative.

3.1.4. Using Social Networking Sites to engage with Communities

Some employees of the Council need to communicate and engage with children and young people and other customers as part of their work. Social networking sites represent an opportunity for such engagement.

However, there are risks associated with using these sites and employees wishing to use this method of engagement, should undertake a thorough risk assessment before doing so. For assistance contact the ICT Service Desk.

3.2. E-mail.

The council considers the provision of e-mail to be a critical business system, therefore responsible use is encouraged by all. Before you send any email consider that it is a public record in the same way as a letter or memo is and may be disclosed under the Freedom of Information Act.

All email usage is subject to logging and monitoring for viruses, malware and compliance to acceptable usage policy.

Managers are responsible for monitoring email use of their staff. If managers have concerns regarding email use, then management information can be provided by ICT Services subject to approval by Internal Audit in accordance with HR and Internal Audit processes.

Intranet link: A guide to email security is available on the intranet:
https://www.havering.gov.uk/intranet/CHttpHandler.ashx?id=12076&p=0

Any employee who accesses or attempts to access another user's mailbox without either management or employee authorisation, or following termination or suspension of employment, may be subject to disciplinary procedures.

Any improper use of internal email, as defined in this policy or otherwise, may be considered by the Council to be a disciplinary matter.

Any attempt to logon using another person's ID may be regarded as a disciplinary matter.

At the request of the manager your email account and Calendar should be set to allow your line manager appropriate read only proxy access to your account.

Where absence is unplanned and therefore unexpected, requests for access to an absent employee's email account must be made by the employee's line manager inline with the current ICT protocol to the ICT Service Desk.

In order to protect the security of the Council's Information assets and to comply with the Government's Code of Connection standard, staff are prohibited from configuring an email rule that **automatically** forward emails from their work email account.

GCSx email account users (e.g. Benefit Services) are also prohibited from configuring automatic forwarding rules from their GCSx account to their havering.gov.uk email account.

Personal information, sensitive information or information marked as "PROTECT" or "RESTRICTED" received via the GSI network must in no circumstances be emailed to an email address(es) outside of those authorised for use on the Government Secure Intranet.

Personal information, sensitive information or information marked as "PROTECT" or "RESTRICTED" held outside of the GSI network by the Council, can be sent externally via a Council email address, providing:

1. That information needs to be sent via email to support a valid business case,
2. The file(s) to be sent is encrypted in line with the Council's encryption standard,
3. The transfer has been endorsed by the appropriate Business Unit Manager,
4. The transfer is authorised by the Group Director of ICT Services (or delegated officer), and
5. The member of staff who is transferring the file maintains a log of the transfer and authorisation within the relevant application/business area.

Where an individual has initiated a request to receive the personal information that the Council holds on them via email, this can be sent via a Council email address to them, providing:

1. Their identity has been verified,
2. A log of the request and disclosure is maintained.

3.2.1. Business use

You **MUST**:

- Set a password on your email account. *See 3.7.3 Security section for information on passwords*.
- Mark emails that you (e.g. Benefit Services) intend to send via the GSI network that contain personal or sensitive information as “PROTECT” or “RESTRICTED” (depending on the sensitivity of the information to be sent). To do this you must start the subject line with “PROTECT” or “RESTRICTED” as appropriate.
- Mark large files for extensive distribution as delayed using [d] at the beginning of the subject line, this will delay the send until late night.

You **MUST NOT**:

- Encourage or promote activities which would, if conducted, be illegal, unlawful or that may breach current policies including anti-minority views, racial abuse, bullying, offensive or sexual harassment.
- Send email that might be defamatory or incur liability on the part of the Council or adversely impact on the public image of the Council.
- Use the Council’s email facilities to deliberately propagate any virus, worm, Trojan horse or known hoax.
- Reply to, or forward chain mail or unlisted junk mail just delete it.
- Send external emails with file attachments larger than 25mb or send emails with file attachments of larger than 20mb to multiple external recipients, as large attachments (over 25Mb) can cause the system to fail and jeopardise email delivery. If in doubt please contact the ICT Servicedesk for advice and guidance.
- Use email marked as personal to disguise business email for any reason.

3.2.2. Personal use

Personal use of the e-mail system is privilege and not a right and should be viewed as such by all users. Remember that the business use rules also apply to personal use of the Email systems.

The reasonable use of Personal emails during the working day is allowed, but should not impact on your working performance/productivity. Personal emails should normally be composed and sent during your own personal time.

Personal use should not affect your or any others ability to carry out Council duties if using the email system for personal use during the working day.

You **MUST**:

- Start the subject line of an email with [P] or Personal if you want the Council to normally treat it as a personal email, no other marking will be considered as personal. Unless information is legally exempt from disclosure, the privacy of emails marked as personal cannot be guaranteed as the information is residing on the Council's computers. While personal information is generally exempt from release under the Freedom of Information Act, a decision to release may be made if the information is considered to be in the public interest. The Council has the right to examine emails marked personal if it reasonably suspects that the contents might contain evidence of criminality, unlawful actions and/or breach of the Council's policies. The personal emails will be accessed **only** by Internal Audit in accordance with HR and Internal Audit processes.

You **MUST NOT**:

- View emails that are marked [p] or are clearly marked as personal when proxy accessing someone else's email account.
- Use email to distribute any material that may be considered to be indecent, **obscene, offensive or abusive to others** in that its content **may** be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful.
- Send email that supports or encourages the committing of illegal acts, refer to or comment on colleagues and managers in a defamatory or slanderous nature.
- Send attachments on personal emails, i.e. photographs, images etc, as excessive volumes of photos & images can cause the system to fail and jeopardise corporate email delivery. If in doubt please contact the ICT Servicedesk for advice and guidance.
- Use email marked as personal to disguise business email for any reason.

3.3. Procurement

Managers must ensure that all ICT hardware/software and Telecommunications equipment purchasing is coordinated through ICT service Desk and purchased via Business Systems Procurement, ensuring that equipment in use across the Council is consistent, meets appropriate standards and is compatible with existing equipment and network resources.

Managers should ensure that users are aware of insurance arrangements and the user's obligations before allowing mobile devices such as laptop computers to be taken off the premises.

Managers should ensure that records are maintained which detail their mobile devices (such as laptop computers) including type, serial number, and include provision for signing out and return.

Managers should ensure that only software for which the Council is licensed is installed upon any Council computer. However, this is assumed to be correct if installation is arranged through ICT service desk, which will retain records relating to current licenses and software packages in use.

3.4. Telecommunications

You **MUST**:

- Adhere to the Telecommunications Protocols Document available from the Telecommunications Services Team and on the intranet:

Intranet link: The Telecommunications Protocols Document is available on the intranet: https://www.havering.gov.uk/intranet/index.aspx?articleid=10323

- Pay for all personal calls identified by users from the 3-monthly call logger reports which are sent out via email.

You **MUST NOT**:

- Be abusive or use sexist, racist, homophobic or religious slurs.
- Use over 18's, chat lines, date lines or any premium rate or 0990 number.
- Discuss 'RESTRICTED' or sensitive Council information over the telephone or face-to-face in unsecured or public areas. If in doubt please see information and guidance on the ICT pages on the intranet. TBA.

3.4.1. Mobile Telephone Specifics

You **MUST**:

- Adhere to the Telecommunications Protocols Document referred to above.
- Comply with current UK Law for mobile use.
- Pay for all personal calls/Text shown on the 3-monthly mobile phone bills sent out as hard copies to Heads of Service.
- Report loss, theft or damage immediately to the Telecommunications Services Team on (43)2520 or (43)2866.

You **MUST NOT**:

- Download new ring tones, colour themes, screen savers or any other software to your Council mobile phone.
- Physically change or modify your Council mobile phone.
- Transfer this phone to another Council user unless the correct paperwork has been completed first.
- Sign up for any extra services.

3.4.2. Voicemail System

You **MUST**:

- Adhere to the Telecommunications Protocols Document referred to above.

3.5. Personal Computers

The term personal computer covers all ICT computing & telecommunications equipment including (but not exclusively) Desktop PCs, Laptops, Tablet PCs, PEDs (Personal Electronic Devices), Blackberrys and mobile phones. All ICT equipment supplied to users is the property of Havering Council.

The Council has the right to seize any Council issued computer equipment & telecommunications equipment at any time.

You **MAY**:

- You may change the screen resolution, colour depth and theme, in order to allow for a more usable working environment.

You **MUST**:

- Store all Council related non sensitive working documents on the network S: Drive. Local drive (C:, E: etc) should not be used for storing working documents".
- Only store files that are work related but are of a private or sensitive nature such as staff PDPAs and require restricted access protection on the U: drive.

You **MUST NOT**:

- Change, amend or adjust any settings and/or configuration of the Council supplied computer equipment.
- Install any software on Council provided computer equipment.
- Use council equipment for the storage and distribution of personal information files.
- Remove software installed by Business Systems.
- Attempt to shut down, circumvent or disable any software installed by Business Systems.
- Install any hardware, either external or internal, that has not been sanctioned and supplied by Business Systems.
- Connect personal USB devices such as iPods, memory sticks, digital cameras, Tom-Toms or mobile phones to LBH equipment.

3.5.1. Mobile Computers Specifics/Working Offsite

As a mobile worker you are required to return your Council supplied laptop/device to ICT for maintenance, updates and Audit purposes on demand.
It is the user's responsibility to ensure the safe keeping of the equipment and any records or information stored on it.
Before and while transporting a laptop or any portable PC equipment:

You **MUST** ensure that:

- A Council supplied VPN client or 3G connection must be used when connecting to Council systems from remote sites.
- The equipment is protected using only LBH sanctioned encryption software & is password protected.
- The equipment is properly packed into an appropriate carrying device i.e. a laptop bag.
- The equipment is properly powered down before transport.
- The DVD/CD ROM drive is properly closed and that nothing is sticking out of the laptop prior to packing it away as per the manufacturers instructions.
- Any mobile computer equipment is stored out of view in an unattended car.
- The equipment in your safe keeping is covered by your insurance while on loan at your home location and when in transit.
- When not in use the equipment is stored in its proper protective carry case and stored securely.
- You report any fault, damage or loss of the equipment immediately to the ICT Service Desk.

You **MUST NOT**:

- Connect ICT supplied equipment to public wireless networks such as available from Internet Cafés as these networks are completely out of the Council's control and therefore un-trusted, insecure and pose too great a risk to our systems and information such as data theft and viruses etc. For use of wireless networks at business conferences in hotels, conference centres and similar locations, please contact the ICT Servicedesk prior to the event you wish to attend in order to ensure that your laptop has the appropriate security measures including encryption, and it is capable (i.e. it is of sufficient technical specification) of using external wireless networks. When at the event you will need to speak to the organisers to get any login credentials that you will need to enable you to access their wireless system.

3.5.2. Health and Safety

You **MUST**:

- Refer to the advice and guidance available from the Corporate Health & Safety Team and on the intranet:

Intranet link: Health and Safety documentation is available on the intranet: https://www.havering.gov.uk/intranet/index.aspx?articleid=5600

You **MUST NOT**:

- Remove the external casing or in any way disassemble or dismantle any computer equipment.
- Move, lift or physically shift any non-mobile computer equipment.

3.6. Remote Access

The Council understands the need for a flexible approach to working, and the need for a fair work life balance. The Council has made it possible for some employees to work at home or offsite at convenient locations via the use of remote access to Council ICT systems. In order to take advantage of these facilities, users must follow these rules.

3.6.1. Working at home

All current Business Systems policies remain in place and the user agrees to abide by them when working off-site from home or any other location. IT equipment supplied by the Council should only be used for Council business, in line with the following conditions:

You **MUST**:

- Ensure that any Havering work documents are **only** stored on LBH sanctioned devices with encryption.
- Refer to the advice and guidance available from the Corporate Health & Safety Team and on the intranet:

Intranet link: Working from Home and Homeworking Code of Practice is available on the intranet:
https://www.havering.gov.uk/intranet/CHttpHandler.ashx?id=2499&p=0

- Use Council approved remote access products with your own personal equipment to remotely access the Council's computer systems (**but not to access GCSx/RESTRICTED resources, systems and data**) on your home broadband connection, wired or wireless, with an RSA token and Citrix Secure Gateway, providing you have up to date antivirus installed. For guidance regarding securing your personal computer equipment please see the following internet link:

Internet link: Get Safe Online: http://www.getsafeonline.org/

You **MUST NOT**:
• Allow other persons to gain access to Council ICT systems or equipment.

You **MAY**:
• Use an **ICT supplied laptop** to remotely access the Council's computer systems (including GCSx/RESTRICTED resources, systems and data which must **ONLY** be accessed from an ICT supplied laptop) on your home broadband connection, wired or wireless, with an RSA token and Citrix Secure Gateway, providing the laptop is encrypted and has all ICT supplied security measures installed.

3.7. Security

The Council has invested a great deal of funds and resources into its computer systems and the data held on it. Therefore it is important to ensure that the equipment and the data stored upon it are kept secure and safe.

3.7.1. Network Access Control

The creation of all new user accounts is carried out by ICT Service Desk on receipt of a new user form detailing the appropriate access levels and permissions by the relevant line manager.

Access to systems and applications is restricted according to the role and business requirements of each user. Access rights are established and managed on a need-to-know basis, and agreed by a user's line manager and the owner of the system or application.

An appropriate manager must always authorise external 3rd party access to and use of the network, which must be by named individuals. Access will only be permitted on completion of a Code of Connection by the manager and the authorised user.

If access to a file held in an individual's U Drive is necessary and that person is not available, e.g. they are off work sick, then the line manager must contact the ICT Service Desk for assistance.

It is incumbent on line managers to ensure that all staff with network access on long term leave and those staff who have left, are immediately reported to the ICT Service Desk. Their email and user area will be archived and removed in accordance with ICT Service Desk procedures, (note, the content of any shared areas will be unaffected).

3.7.2. Equipment

You **MUST**:

- Keep Council issued equipment safe and secure, it is your responsibility.
- Report any theft, loss or damage to Council issued equipment to the ICT Service Desk immediately.

You **MUST NOT**:

- Allow any non-Council employee to access Council equipment and resources with Council issued equipment.

3.7.3. Log in

You **MUST**:

- Set your password to at least 8 characters in length and contain at least 1 uppercase alpha, 1 lowercase alpha, and 1 numeric character e.g Perm1TT3d or £a514T26.
- Contact the ICT Service Desk for assistance if you forget your password, or if you suspect it has been discovered.
- Must lock the pc or log out completely if you leave your pc unattended for any length of time.

You **MUST NOT**:

- Write down your user name and password.
- Share your user name and password with anyone else.
- Allow other users to log in with your username and password.

3.7.4. Data

Managers must ensure all staff are aware of their responsibility to safeguard the security of all data for which they are responsible, or which they access to carry out their job. It is also staff's responsibility to bring to their manager's attention any areas of concern regarding the transfer or transportation of sensitive or confidential information.

Managers must authorise or prohibit the disclosure, transferal or copying of confidential, personal or sensitive information by their staff.
Staff must not disclose, transfer or copy confidential, personal or sensitive information without the express authorisation of their manager and the authorisation is to be recorded.

Personal information, sensitive information or information marked as "PROTECT" or "RESTRICTED" received via the GSI network must in no circumstances be emailed to an email address(es) outside of those authorised for use on the Government Secure Intranet.

Intranet link: Government Connect Programme training:
https://www.havering.gov.uk/intranet/index.aspx?articleid=16663
When transferring data to 3rd parties, users are advised to read and comply with the guidance publish on the intranet.
Intranet link: Secure Information Transfer:
https://www.havering.gov.uk/intranet/index.aspx?articleid=12455
Intranet link: Information Sharing Protocol:
https://www.havering.gov.uk/intranet/index.aspx?articleid=11616

You **MUST**:

- Ensure that Council data is stored using only ICT approved encrypted devices.
- Ensure data stored locally or on any form of storage device for transport or working off line, is returned and stored on the network a soon as possible.
- Once information has been transferred to the Council's network, delete the local copy.
- Keep a log of what the data is if you are removing or transporting data of any type.
- Report the loss of data, security incident or breach immediately to the ICT Service Desk.
- Wherever possible store all data on the Council network and not on local drives or other storage devices.
- Report any anti-virus warning messages or actual virus attack to the ICT Service Desk immediately.

You **MUST NOT**:

- Use standard e-mail to transmit documents of a highly confidential nature or that contain personal or classified information.
- Use unsanctioned or unencrypted USB key drives or CDs and DVDs etc to transport or store confidential, personal, sensitive, or classified information.
- Discuss or disclose any data in your safe keeping, unless it is as part of your normal day to day working practices.
- Discuss or disclose any data to any unauthorized party.

You **MAY**:

- Divulge confidential or sensitive data in your safekeeping, if you need to disclose the information as part of the 'whistleblower' process and you are following properly the 'whistleblower' procedure set down by the Council.

4. Who Is Covered By This Policy?

Any reference to user(s) within this policy applies to all Council employees, contractors, sub contractors, agency staff, partner organisations, third party's or elected Members who have access to, or use any Council information, communication or computer equipment. All managers are responsible for the implementation and policing of the Policy.

In respect of contractors and other users, breaches of the policy could lead to systems access being withdrawn or other action being taken.

Managers should use the policy to create and maintain a level of awareness of the need for ICT and information security to be an integral part of day to day operations and the responsibility of all staff to comply with this and other relevant policies.

5. What Is Covered By This Policy?

All Information held by the Council in all formats whether it is hand-written or printed, held in an electronic format, such as email, Microsoft Office Products, digital audio or video, analogue audio and video, microfiche, database, or any digital or non digital format. Examples of this are procedures, policies, draft documents, minutes of meetings, agendas, emails, leaflets, forms, photos, videotape, mp3, mpeg, avi, wmv etc.

Voice and data communications equipment. Examples of this are Council telephone extensions, mobile telephones, Blackberries, routers, hubs switches, PABX's, 3G, GPRS, etc.

All personal computers. Examples of these are desktops, laptops, tablets, note books, PDA's, Blackberries.

PLEASE NOTE: A number of Corporate workstations (PCs and laptops etc) now have the ability to be used as communications devices. It is therefore important when you read this policy to take this into consideration.

6. Exemptions to This Policy:

Business Systems support teams comprising: PC support, Network and Servers support, Information Security Team and Corporate and

Business Applications only. – Insofar as the normal day-to-day operations carried out as part of their duties e.g. the loading of software.

7. Seeking an Exemption:

Any user, group, section or service may seek an exemption to part of this policy in order to carry out a specific business purpose. All requests for exemption must be registered with the Business Systems ICT Service Desk in writing for approval by business systems. Requests may be rejected if there is not a credible business case for the exemption with Head of Service or Group Director Support.

8. What Happens If This Policy Is Breached

Managers must ensure that any individual who becomes aware of a security incident, weakness or violation must report it as soon as possible to the ICT Service Desk

8.1. What is considered a breach of this policy?

The policy will be considered breached if any one or more of the rules are not adhered to.

8.2. How will breaches be dealt with?

Any security breach or violation of this and other related policies could lead to appropriate action being taken against those responsible. A full investigation will be carried out, which may result in disciplinary action being taken against staff. In cases of gross misconduct this may result in dismissal. Gross misconduct may include but is not limited to excessive personal use of email, inappropriate emails, and personal use of the internet during working hours and accessing inappropriate websites. This is not an exhaustive list.

In respect of Members a report may be made to either the Standards Board for England or the Council's own Standards Committee depending on the Code or Protocol breached.

In respect of contractors and other users, breaches of the policy could lead to systems access being withdrawn or other action being taken.

As part of that investigation process, access to a user's login, email account and the forensic examination of file contents may be required. This will only be possible with the explicit written permission of the Head of HR, the relevant Head of Service, who will authorize Internal Audit and the Investigating Officer access rights.

If you are unsure of any aspect of this policy or require clarification then you must contact your line manager or the ICT Service Desk.

8.3. How will people be advised of the policy?

All current users will be regularly reminded of the policy and its content via global email\citrix\intranet and internet disclaimers and other methods.

New users will receive a copy of the policy in the New Starter Induction Pack, as well as the policy being placed on all new PCs deployed, is published on the Council's intranet and sent as part of a welcome email to all new GroupWise accounts. Contractors and other party's working for the council must also receive a copy of this policy; this is the responsibility of the line manager/Head of Service.

Intranet link: This policy:
https://www.havering.gov.uk/intranet/CHttpHandler.ashx?id=8449&p=0

8.4. Applicability to Council Members

Restrictions on the use of resources is imposed on Members by this policy and the Members' Code of Conduct and the Protocol on Member/Officer Relations which provide that resources may not be used for political or party political activity or for campaigning. **Members' attention is drawn to paragraph 28 of the Protocol on Member/Officer Relations in respect of the use of Council resources.**