Internet, Email and Social Media Policy and Guidance

February 2016

London Borough of Tower Hamlets

VERSION CONTROL

Version	Date	Author	Description
0	13/07/2015	Allan Caton	*Initial draft created*
0.1	24/09/2015	Allan Caton	*Document amended to clarify permissible Internet usage*
0.2	21/10/2015	Allan Caton	*First full version – Draft*
1	02/12/2015	Allan Caton	*First full version - Final*

Approved: **Date:**

Zena Cooke, Corporate Director of Resources, (SIRO) **2nd February 2016**

TABLE OF CONTENTS

1. SUMMARY

The London Borough of Tower Hamlets (LBTH) recognises that e-mail, the internet, intranet and social media are essential business tools for communication, creating, storing, accessing, processing and transferring information, with instant messaging having become important for internal communications. The Council invests substantially in information technology and communication systems and recognises that they play an essential role in delivering Council services.

This policy and guidance sets out the principles for the acceptable use of these facilities and guidance on best practice taken from the internationally accepted code of practice for Information Security – ISO/IEC-27002.

This policy forms part of the Council's information governance framework. It should be read in conjunction with the following –

- Information Security Policy
- ICT Acceptable Use Policy
- Data Protection Policy
- Email and Internet Guidance

The Internet and Email Policy and Social Media Guidance is a high level document. Reference is made throughout the policy to related policy and guidance material which supports the implementation of this policy. All staff and those who work for or on behalf of the Council must read and adhere to all related policy and procedures (Appendix 3).

Back to Top

2. OBJECTIVES

The Council is committed to ensuring the confidentiality, integrity and availability of it's information assets. The Internet and Email Policy and Social Media Guidance is designed to help ICT users understand the Council's expectation for the correct use of these resources. The aims of this policy are to:

- Encourage usage that supports the business goals and objectives of the Council
- Protect the Council's data, systems and equipment
- Ensure that all employees are aware of and understand this policy and discuss with their manager if there are any parts which they do not understand
- Ensure that internet, email and social media use complies with Council policies and UK and European law
- Prevent misuse of the internet, email and social media
- Explain that failure to follow this policy could result in disciplinary action

Back to Top

3. DEFINITIONS

A glossary of terms used in this document is listed in Appendix 5.

The terms '*ICT users*', '*staff*' and '*employees*' when referred to in this document, relates to all full time, part time, casual and agency staff, home workers, contractors, 3rd parties and any other person(s) accessing the corporate network.

Back to Top

4. POLICY

4.1 EMAIL POLICY

Use of email by ICT users of the London Borough of Tower Hamlets email system is permitted and encouraged where such use supports the goals and objectives of the business.

However, the London Borough of Tower Hamlets has a policy for the use of email whereby the employee must ensure that they:

- comply with current legislation
- use email in an acceptable way
- do not create unnecessary business risk to the Council by their misuse of email

Unacceptable Behaviour

The following behaviour by an employee, whilst not an exhaustive list, are examples of what is considered unacceptable and can be considered as gross misconduct:

- use of Council communications systems to set up or run personal businesses or send chain letters
- forwarding of confidential Council messages to external locations including personal email addresses or personal cloud storage locations
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive in that the context is a personal attack, sexist or racist, or might be considered as harassment or which describe techniques for criminal or terrorist acts.
- accessing copyrighted information in a way that violates the copyright
- breaking into the Council's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- knowingly introducing any form of computer virus or malware into the corporate network

Monitoring

The London Borough of Tower Hamlets accepts that the use of email is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the Council's email resources are provided for business purposes. Therefore, the Council maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the Council also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with the ICT investigation procedure. Where appropriate LBTH reserved the right to contact relevant authorities such as the Police.

Back to Top

4.2 SENDING OR RECEIVING INTERNAL EMAIL

You must:

- Check your in-box regularly (usually at least 3 times per day)
- Make sure that messages you send are clear and unambiguous
- Ensure e-mails are not sent without text in the subject line
- Never send an email out of anger – ask a colleague to 'sanity check' the email before sending
- Be aware that the inappropriate use of upper case in e-mail is generally interpreted as SHOUTING and should be avoided
- Set an "Out of Office" message on if you are going to be out of the office for one day or more. This must include the dates when you will be away, when you will be returning, and an alternative e-mail and contact telephone number: For example:

  > I will be out of the office from Monday 7th March until Thursday 10th March and will reply to your e-mail when I return on Friday 11th March. If your enquiry is urgent, please contact *Colleague Name* on *020 7364 XXXX*, e-mail colleague.name@towerhamlets.gov.uk. Thank you

- When sending an e-mail to several people, make it clear who needs to take each action. Consider each proposed recipient individually. Only use the (CC) carbon copy when you do not want an individual to take further action but you do want them to be aware of the contents of the e-mail
- Use the Carbon Copy (CC) facility wisely – do not copy in senior staff or managers to prompt a swift response unless an escalation is required. This can be construed as a form of bullying and can lead to unnecessary antagonism in the workplace
- Only use the "urgent" indicator when justified
- Be very careful not to set unreasonable time scales and deadlines without discussing the impact with the individual. The recipient may be on leave and unable to act on the message
- Be very careful if you use Blind Carbon Copy (BCC). People that you e-mail may use "Reply All" but will not be aware of who all the recipients are
- Be careful not to misuse 'read receipt' to pressure the receiver into action
- Remember that attachments can be lost using the reply feature – use the forward feature if attachments need to go to others
- Do not send attachments which are available via the corporate network, send the location instead. Where attachments are required ensure that they are compressed wherever possible

\...Continued

- You should perform regular housekeeping on your mailbox to ensure that the contents remain below the 100Mb limit. This can include emptying your 'deleted items' folder, archiving emails no longer required using Enterprise Vault, deleting unwanted or un-needed emails, saving large attachments to a network share and deleting the original email and setting up email folders which can be archived on completion of work

- Avoid attaching chains of correspondence to external people as this can look unprofessional. Where an email trail is required ensure it does not contain information you did not intend to forward

- Remember that all business related e-mails may be disclosed under the Freedom of Information Act 2000

- Be aware that there should be no automatic expectation of privacy when using the corporate email system. Avoid sending emails which you would not want to be disclosed or which could cause embarrassment to yourself or others.

- Use an Auto Signature at the bottom of the e-mail following the corporate standard. You must not add extra text, disclaimers or images to your Auto Signature. To set up your Auto Signature select the Auto Signature options from the Tools menu and follow the instructions. The corporate standard is:

- Your full name
- Your full job title
- Your section
- Your directorate
- London Borough of Tower Hamlets
- Phone: your phone number including full area code
- Fax: your fax number
- E-mail: your full e-mail address
- Website: http://www.towerhamlets.gov.uk
- Your complete address including postcode

Back to Top

4.3 RESPONDING TO EMAIL FROM MEMBERS OR EXTERNAL BODIES

Corporate complaints procedure and the Members enquiry procedure takes precedence over the regular e-mail standards see ("Standard when sending or receiving e-mails") where a complaint or Members enquiry is contained in an e-mail.

Where you are responding to public enquires from external people or business, you must:

- Abide by all of the standards set out for internal email and:
- Remember that in line with the Implementing Electronic Government (IEG) Statement, the Council is committed to responding to all public enquiries by e-mail that are sent to generic e-mail addresses i.e. helpdesk@towerhamlets.gov.uk, in full within 24 hours.
- Remember the Customer Promise (for e-mails not sent to generic e-mail addresses) that the Council is committed to responding to all public enquires by e-mail in full within 10 working days. This is the same standard as for letters.
- Send an acknowledgment if you are unable to answer an e-mail within 5 working days telling the customer why and when they can expect a full reply.
- Allocate a unique reference number with all e-mail and web form acknowledgements to allow tracking of enquiry and service response.
- Ensure that only a single notification is required of a change of address i.e. a citizen should only have to tell the Council they have moved on one occasion and the Council should then be able to update all records relating to that person to include the new address.

Although the Council treats e-mails in the same way as letters, the Council recognises that people often expect a faster response. You may find it helpful to acknowledge e-mails more quickly advising senders of when they can expect a full response to avoid them sending further e-mails to chase progress or phoning you to confirm receipt.

A public enquiry by e-mail is a written message addressed to an organisation or person from an identified source that requires an action or response. The first named recipient of e-mails is the person who is required to respond.

If you receive an e-mail that should be dealt with by another Directorate or section, you should respond to the person who e-mailed you and to inform them who the correct contact is and explain how they can get in touch with them. You should include the correct name, e-mail address and telephone number. You should carbon copy (CC) the correct contact into your response if they have an e-mail address or send them a hard copy of the original email.

Back to Top

4.4 INTERNET POLICY

Use of the internet by employees of the London Borough of Tower Hamlets is permitted and encouraged where such use supports the goals and objectives of the business. Occasional and irregular personal use of the Internet is permitted before 09:00 and after 17:00 but should be kept to an absolute minimum between 09:00 and 17:00 due to the adverse effect on the corporate network speed.

However, the London Borough of Tower Hamlets has a policy for the use of the internet whereby employees must ensure that they:

- comply with current legislation
- use the internet in an acceptable way
- do not create unnecessary business risk to the Council by their misuse of the internet

Unacceptable Behaviour

The following is not an exhaustive list but are examples of behaviour which is deemed unacceptable by employees and can be treated as gross misconduct:

- visiting internet sites that contain obscene, hateful, pornographic or that describe techniques for criminal or terrorist acts or otherwise illegal material
- Any form of gambling over the internet
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence and ICT approval has been obtained
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about the London Borough of Tower Hamlets, your colleagues and/or our customers
- undertaking deliberate activities that waste staff effort or networked resources
- knowingly introducing any form of malicious software into the corporate network

Council-owned information held on third-party websites

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of the London Borough of Tower Hamlets. This includes such information stored on third-party websites and corporate social networking sites, such as Facebook.

Monitoring

The London Borough of Tower Hamlets accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business and may result in the facility being withdrawn from individual users.

In addition, all of the Council's internet-related resources are provided for business purposes. Therefore, the Council maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Back to Top

4.5 SOCIAL MEDIA GUIDANCE

This section of the policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

The non-business use Social Media sites from a corporate device is not allowed. (Please refer to the corporate Social Media Policy)

The following principles apply to personal use of social media when referencing the Council as well as corporate use of social media on behalf of the London Borough of Tower Hamlets. In addition to the guidance below employees accessing corporate social media sites should also refer to the corporate Social Media Policy, owned by the Communications Team.

- Staff should be aware of the effect their comments may have on their reputation as well as that of the Council. The information that employees post or publish may be public information for a long time and may be re-posted by others
- Staff should be aware that the Council may observe content and information made available by employees through social media. Where this content is deemed to be in contravention of the LBTH Code of Conduct appropriate disciplinary action may be invoked
- Staff should not directly identify another staff member or any personal details without express permission of the staff member being referenced unless there is a business requirement to do so.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content or images that are defamatory, pornographic, proprietary, harassing, libellous or that can create a hostile work environment
- Employees are not to publish, post or release any information that is considered confidential, sensitive, inflammatory or private. If there are questions about what is considered confidential, sensitive, inflammatory or private employees should check with the Human Resources Department and/or their line manager.
- Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- If employees publish personal content that involves work or subjects associated with LBTH, a disclaimer should be used, such as: “This post is my own and may not represent the London Borough of Tower Hamlets positions, strategies or opinions.”. The use of a disclaimer, however, will not indemnify the user against disciplinary action should the post be deemed to be inappropriate. A disclaimer such as the one above can be used in the ‘Intro’ or ‘About’ section of personal media pages.

Back to Top

4.6 INTRANET GUIDANCE

The Council has developed its own Intranet site to provide easy access to relevant information for its employees. The Council encourages all employees to access the intranet.

The intranet provides a range of useful information including:

- Current news
- Staff telephone directory
- An A – Z of Council services
- Services within the Council
- ICT Service Desk call logging system
- HR Policies and Procedures
- Employment policies and procedures
- Committee reports

Each service area will have a nominated person who is responsible for updating information on the intranet. They will receive training in order to do this. You should notify this person if you notice that a page needs updating.

Back to Top

4.7 OTHER MOBILE DEVICES

Council issued mobile phones, Blackberrys and Personal Digital Assistants (PDAs) capable of accessing the Council network are covered by this policy. Personal equipment used in the course of working for the Council is also covered, for example a personal mobile device accessing email via DME.

Using DME on a mobile device you will have access to corporate email (but not GCSX), your calendar and associated MS Outlook functions. Care should be taken to ensure that the information displayed on the screen of your mobile device cannot be overlooked.

Back to Top

4.8 INSTANT MESSAGING

Instant Messaging (IM) is a tool, like email, that allows a form of text based communication from one person to another person or group. It is a vital component of the Council's Smarter Working strategy with the emphasis being what you do, rather than where you do it.

IM operates on a real time basis, meaning that as long as the required persons are connected to the Instant Messaging server, each person is able to see the connection status of the other and communicate with them almost instantly. You can find people, see information about their availability, and communicate with them instantly using the most appropriate method; please note IM is not an appropriate channel for communicating with Elected Members. Like a phone conversation, IM allows users to 'chat' back and forth in real-time.

There are several benefits of Instant Messaging:

- The availability i.e. the 'presence' of users indicated by IM, provides near instant communication;
- Avoiding unnecessary email messages which saves time; and
- Cost savings by reducing email communication for simple messages therefore requiring less disk storage.

Acceptable Use

- The council supports the use of IM for work related activities for short and immediate communication. It is not a replacement for Email; rather an enhancement that helps to improve immediate communication using short messages.
- IM is not an appropriate channel for communicating with Elected Members.
- Employees are expected to use IM responsibly, and only use where instant responses are required as long as the person has signified they are online.
- IM should primarily be used for work related purposes only. Reasonable and limited use for personal purposes is acceptable, provided that this use does not affect individual productivity and work. Wherever possible, personal use should be in the individual's own time.
- All policies and guidelines pertaining to information security and email content also apply to IM, including, but not exclusive to, policies regarding solicitation, obscenity, harassment, bullying, inappropriate communication, pornography and sensitive information.
- IM should be used to effectively manage interruptions and involvement in IM discussions e.g. use busy, if you do not want to be interrupted.

\..continued

Security

- IM traffic is not encrypted, therefore sensitive data, such as username, passwords, account numbers and other personal data should not be passed via IM as it could be read by other parties other than the intended recipient(s). Transferring sensitive data using IM is not allowed.
- File sharing or downloading files is prohibited.
- IM must not be used for communicating financial information, decisions, historic or other information that must be retained for statutory or Council purposes.
- All IM communications will usually be automatically deleted when the conversation is closed.
- If records of IM conversations are made (i.e. if the conversation is printed or copied and stored electronically), they are subject to the Freedom of Information Act, Data Protection Act and Environmental Information Regulations (just as if they were emails or memos etc), and the information is held at the time of the request being received by the Council.
- IM conversations are not stored; however, usage is periodically reviewed to ensure compliance with this policy. Management information about usage is held by the system.

Monitoring

- Monitoring will be conducted whenever senior officers or Internal Audit deem it necessary.
- Users of IM should have no expectation of privacy. The council reserves the right to monitor, review and investigate individual IM activity and use of the council's equipment and network.
- Any monitoring is in accordance with the Council policies and may include: excessive use or abuse during the workday and to detect violations of the Council's policies.

Back to Top

5. POLICY SCOPE

All ICT users covered by this policy must read this policy, the Information Security Policy, the Acceptable Use Policy and Security Manual, to ensure they have an understanding and are familiar with the expectations and their responsibilities. You should also read this policy in conjunction with the Council's Home Working Policy and Flexible Working Policy, where applicable.

Where it is believed that an employee has failed to comply with this policy, they will face the Council's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

Back to Top

6. MANAGERS RESPONSIBILITIES

As a manager you must:

- Monitor your staff and ensure they are using e-mail/internet/social media appropriately.

- Ensure your staff are aware that they can only use facilities for personal use before the start of the working day, during authorised breaks or after the end of the working day and only within the guidelines set out in the Information Security Policy, Acceptable Use Policy and Email, Internet and Social Media Policy.

- Inform your staff that if they abuse the privilege of using e-mail/internet or personal use, this may be withdrawn at any time and they may be subject to disciplinary procedures.

- Investigate any apparent misuse of the Council's e-mail, internet and intranet facilities and notify Human Resources and ICT. Please refer to the ICT Investigation Procedure in Appendix 1

- Investigate any e-mails containing offensive material which are brought to your attention and notify Human Resources and ICT. Please refer to the ICT Investigation Procedure in Appendix 1

- Ensure that if any of your staff are working off site that they use the Council's VDI system to access corporate resources such as email and corporate ICT access. Under no circumstances should personally identifiable data be sent to an account or e-mail address outside of the council network unless secure e-mail capabilities exist.

- Make sure your employees are aware that it is strictly prohibited to use USB sticks, CDs or memory storage devices on the Council's computers or laptops.

Back to Top

7. EMPLOYEES RESPONSIBILITIES

As an employee you must:

- Read and understand the contents of this policy, the Information Security Policy and the Acceptable Use Policy
- Discuss with your line manager any aspects of these policies which you do not understand
- Understand you may occasionally use facilities for personal use before the start of the working day, during authorised breaks or after the end of the working day. Personal use of the internet is a privilege that must not be abused and this can be withdrawn at any time.
- Understand you may be required to justify your use of the internet. If asked to do so and if it is found that you have abused the privilege of using the internet for personal use you may be disciplined.
- Understand that is strictly prohibited to use USB sticks, CD's, memory storage devices on the Council's computers or laptops unless there is a supporting business case which has been approved by the ICT Security and Information Governance Officer.
- Notify your line manager if you receive any unsolicited e-mails containing material which is unlawful, indecent, offensive or inappropriate.
- Notify your line manager if you know or suspect improper use of e-mail or internet. Please refer to the ICT Investigation Procedure in Appendix 1
- Notify your manager if you mistakenly access a prohibited internet site or page that contains material which is unlawful, indecent or objectionable.
- Be aware that the Council reserves the right for authorised personnel to monitor your e-mails and internet usage to assure compliance with all Council policies. Such monitoring will be used for legitimate purposes only.
- Understand that you will be disciplined if you breach the policy or guidelines, which could result in your dismissal and possibly criminal proceedings.

Back to Top

8. EMPLOYEES WITHOUT EMAIL AND INTERNET ACCESS

Some employees do not have access to e-mail or the internet. In such circumstances, managers should use alternative forms of communication to ensure that all employees have access to communications, especially information they need to do their job effectively.

Back to Top

9. IMPLEMENTATION

Confidentiality Agreements

All members of staff will be working to a contract of employment which would include clauses regarding information that they receive in the course of their employment. This requires them to ensure confidentiality of London Borough of Tower Hamlets information during and after their employment with the Council. All employees handling critical or sensitive information must be subject to a formal pre-employment screening, which must include satisfactory professional references. The confidentiality of Council owned information precludes the use of personal cloud storage, personal email (Hotmail, Yahoo, Gmail etc), personal social media accounts and online forums which are not corporately authorised.

Where agency, contract and other third party staff are concerned, a confidentiality agreement is required before they are granted access to London Borough of Tower Hamlet's ICT facilities. Agency contracts and supplier contracts may exist which contain clauses relating to confidentiality, which satisfy this requirement. Where such clauses do not exist, the Information Security Officer should be contacted so that an appropriate agreement can be created.

.

Profile raising and publicity

This policy will be made available to all new staff joining the organisation and on the Intranet and is referred to in Corporate Induction training. Significant updates will be communicated to all staff when the policy is reviewed and refreshed

Compliance

The Complaints & Information Team will work with Service Area appointed Information Governance Group Representatives and Information Asset Owners to establish a programme of work and priorities for Internet, Email and Social Media usage. Compliance with the policy will be monitored and adherence / failure to comply reported to the SIRO.

Audit Reports pertaining to this issue will be discussed at the Information Governance Group and action required to manage risk and matters arising will be actioned.

Ultimately, Government Networks and partners reserve the right to disconnect the Council from their services if security breaches occur or non-compliance with their rules which would severely impact on our ability to efficiently deliver services to the public which often requires close working with partner organisations such as the Police, NHS and Department of Works and Pensions.

Back to Top

10. REVIEW/ SIGN OFF

The adopted Internet and Email Policy and Social Media Guidance on 02/02/2016 will be reviewed annually or sooner if required, for approval by Information Governance Group (IGG) and sign off by the FOI Board, and owned by the SIRO.

Back to Top

Appendix 1 – ICT Investigation Procedure

Investigations under this procedure involving Council employees will be undertaken in line with the Disciplinary or other Council policies. Human Resources or legal services will decide on which policies apply to Councillors or external contractors (including agency staff)

1. Introduction

1.1 There are occasions where the use of ICT by employees, Councillors or external contractors needs to be reviewed or investigated. Typically this is where there are suspicions about the behaviour of an individual – suspected misconduct or fraud, but also where allegations against individuals have been made, for example under the Whistle Blowing procedures.

1.2 The purpose of this procedure is to ensure that any investigations carried out concerning the use of ICT by an employee, Councillor or external contractor is conducted fairly and comprehensively. Investigations of this nature are often sensitive and need careful planning and execution. They are also technically demanding and require a methodical approach. The investigations must therefore be carried out with the utmost confidentiality and diligence.

1.3 This procedure sits alongside HR and Information Governance policies and procedures including the E-mail, Internet and Social Media Policy and the Information Security Policy. It is in line with the Anti Fraud and Corruption Strategy and the Whistle Blowing Charter.

2. Inputs

2.1 There are a number of potential inputs into this procedure. Firstly, proactive monitoring of ICT activities may give rise to a concern – e.g. an individual visiting or attempting to visit restricted sites. A report – either proactively or routinely provided to a manager or human resources would give rise to a requirement for a full investigation about that employee's activities.

2.2 Employees may suspect colleagues of impropriety, e.g. frequently staying late, suspicious activity, closing down screens when employee visits, and holding material on their PCs. This is by no means an exhaustive list. Employees may alert their manager or Human Resources, who may authorize an investigation. In both the above cases, an online form can be filled in which will go to a specific mailbox.

2.3 Under whistle blowing arrangements, it may be that a manager, Service Head or Director are under suspicion. In which cases the whistle blowing policy will direct the whistleblower to a suitable path of escalation. Information received by the whistleblower will need to be passed to the Investigation Co-ordinator in a suitable format to determine if an ICT investigation is to proceed.

2.4 This procedure is concerned with the period of time from the point that an ICT investigation has been determined as being critical to the overall investigation triggered by one of the above inputs.

2.5 It is essential that as much information as possible is provided to support firstly the case for an ICT investigation, and secondly the investigation itself. This will include, and not be restricted to, date of incident, user account, workstation ID, location of activity (location at work, at home, offsite etc..), suspected activity, time, subject of suspected emails, possible file titles etc. The referral form should be completed to the best of the informant's ability.

2.6 If a concern is raised through the whistle blowing route via the whistle blowing hotline the whistle blower will not be expected to complete the referral form. The Registration Officer who takes the whistle blowing call will complete the referral form on their behalf.

2.7 The referral input will be directed to a shared mailbox. Referral forms or emails will be opened by the Registration Officer (RO), logged and allocated a reference number, and then referred to the Investigation Co-ordinator and Human Resources.

3. Determining need and scope for investigation

3.1 The form or e-mailed referral will be passed to the Investigation Co-ordinator (IC). Typically the Service Head for Risk Management as Investigation Co-ordinator (IC) will determine the need for an ICT investigation. Where it is not appropriate, the Assistant Chief Executive (Legal Services) will act as the IC.

3.2 The commissioning of the investigation may follow after a screening assessment. This would consider the nature of the allegation, and whether an ICT investigation was necessary in investigating the allegation. ICT investigations are never to be used as a "fishing trip" to try and find additional material where an allegation has been made, but an ICT investigation is not necessary to prove or disprove that allegation. The IC needs to be satisfied that an ICT investigation is appropriate. If an investigation is appropriate, Human Resources and the employee's line manager should be informed at this point.

3.3 The IC and Line Manager will determine the scope of the investigation. This would direct the investigation to specific activities, timeframes, locations etc. It may be that the investigation should go back 1 week, or may require a lengthier timeframe. Also, the investigation may require priority in terms of a proposed action against the person under investigation (e.g. suspension and/or disciplinary hearing).

3.4 Where there is a genuine concern that the allegation is potentially well-founded and relates to a serious matter and there is a possibility that the individual may attempt to tamper with ICT evidence, consideration should be given to suspension pending an investigation. If, suspension is required, Human Resource will undertake this with the employee's line manager.

3.5 If this action is carried out, their credentials and access rights should be suspended immediately. It may be that to preserve the integrity of the information that the full reasons for suspension are not made apparent to the individual (to avoid others tampering with information on their behalf).

4. Conduct on investigation

4.1 The IC will ask the Information Security Manager to gather the technical evidence. The ISM will be skilled in ICT forensics, or be able to locate sufficient employees to carry out these activities. It may be that, depending on the severity of the allegation, or a perceived conflict of interests regarding the ISM and another employee, external resources would need to be procured to conduct the investigation.

4.2 A log of the activity concerning the investigation should be kept. This will form part of the final report to the IC. All copies of the relevant documents should be sent to Human Resources.

4.3 The IC together with Human Resources may ask other employees to participate in the investigation. For example Information Governance may need to be involved regarding potential breaches of policies. They should only be included where necessary and may not need to know the identity of the person being investigated. The investigation should be carried out with the utmost confidentiality.

4.4 The investigation needs to be completed in a timely fashion. Due regard should be paid to current backup procedures where there is a possibility that information relating to activities would be overwritten e.g. event logs, email logs etc.

5. Feedback to Informant

5.1 During or following the investigation, the informant may call for an update. They may also call to provide additional information e.g. a recurrence of the behaviour that led to the original complaint, or activity which may be an attempt to “cover their tracks”. Care should be taken when feeding back regarding the confidentiality of the material and the individual being investigated. The informant should only be told if action has been taken or not.

6. Feedback to individual where no evidence has been found

6.1 Where individuals ICT activities have been investigated and where no evidence has been found, the IC, Human Resources or employee’s manager should inform the individual at the conclusion of the investigation. This is clearly a sensitive solution and care should be taken to not erode the relationship between the individual, ICT and any internal informant.

6.2 Where an allegation has been made which has not been substantiated, a decision needs to be taken on whether the allegation was false and whether disciplinary action needs to be taken against the informant, if known. However it is essential that overall trust in this procedure is not undermined.

7. Feedback to individual where evidence has been found

7.1 Where an allegation has been made which has been substantiated, the employee’s manager will decide if formal disciplinary action is appropriate, if so, they will notify Human Resources who will arrange a disciplinary hearing, in line with the Council’s Disciplinary policy.

Back to Top

Appendix 2 – ICT Investigation Request Form

This form is to be used by staff to request an investigation of a member staff because of their usage of internet, e-mail, applications or PC. Please note that the form needs to be authorised by Service Head for Risk Management before the request can be actioned.

All parts of the form need to be completed.

Please provide the following details

Name:

Designation:

Directorate:

Location:

Telephone No:

Email Address:

Please provide the reason why it is necessary to monitor the employee's internet/e-mail usage or analyse PC, detailing any particular concerns that you might have.

Please provide the following employee details: Name: Department: Location: PC Asset No.: Telephone No.: Email Address:

The Completed form should be emailed to:
internal.investigations@towerhamlets.gov.uk

Internal use: Authorised by: Authorised by Service Head for Risk Management 1 Where it is not appropriate to seek authorisation from Service Head for Risk Management, the Assistant Chief Executive Legal Services will authorise the request.

Back to Top

Appendix 3 – Supporting Documents

Documents supporting this policy include (this is not an exhaustive list):

Document	Purpose
Clear Desk Procedure	Procedure for all staff to promote flexible working practices
Corporate Business Continuity Policy	Procedure and plan to ensure continuity of business in the event of an incident that affects the availability of information or information systems
Data Protection Policy	Policy sets the standards by which the Council protects and safeguards personal data, complying with the law
Employee's Email and Internet Guidance	Procedure to help employees understand the Council's expectation for the use of these resources and to ensure that they are used correctly
LBTH Acceptable Use Policy	Defines the acceptable use and security rules relating to secure email and information technology systems
Information Handling Procedure	Procedure sets out the requirements for handling Information held by the Council
Information Systems Third Party Access Agreement	Provides a framework for instances where other organisations are invited on LBTH's premises to access LBTH's information systems and network
Email and Internet Policy and Guidance	Policy sets out the principles for the acceptable use of Internet and Email facilities
Protective Marking Scheme	Provides a common baseline and rules for safeguarding information
PSN Acceptable Use Policy	Defines the acceptable use and security rules relating to secure email and information technology systems
Records Management Policy	Policy sets out the Councils responsibilities and activities in respect of managing the entire information lifecycle of its records
Security Incident Management Policy	Policy and procedure for handling security incidents
Smarter Working Policy including : Flexible Office Working Procedure and Flexible Home Working Procedure	Procedures for managers and staff with clear guidance to working flexibly in the office environment and home working
Social Media Policy and Guidelines	Policy and guidelines for managing and regulating the corporate use of social media

Back to Top

Appendix 4 – Legislation and Guidance

Computer Misuse Act 1990

Data Protection Act 1998

Human Rights Act 1998

Freedom of Information Act 2000

Environmental Information Regulations 2004

Electronic Communications Act 2000

Copyright, Designs and Patent Acts 1988

Codes and standards:

- ISO 27001- Information Management Security Management Standard
- ISO 27002 – Code of Practice for Information Security Management
- Public Sector Network (PSN) Information Assurance Conditions
- IgSoc/N3 Code of Connection (For NHS connection and information sharing)
- Payment Card Industry Data Security Standard (PCI DSS)

Back to Top

Appendix 5 – Glossary of Terms

A glossary of terms used in this document is listed below:

Term	Definition
Availability of information	Ensuring that authorised users have access to information and associated assets when required
BPSS	Baseline Personnel Security Standard describes the pre-employment controls for all civil servants, members of the Armed Forces, temporary staff and government contractors generally. The personnel security controls must be applied to any individual who, in the course of their work, has access to government assets.
Confidentiality of information	Ensuring that information is accessible only to those authorised to have access
Corporate Password Policy	The LBTH corporate password policy is as follows: • Minimum of 8 characters • At least one numeric or special character • Changed every 60 days or sooner
CJSM	Criminal Justice Secure Email is intended to provide criminal justice organisations and practitioners to email sensitive and confidential securely
DBS	The Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (ISA) have merged to become the Disclosure and Barring Service (DBS). CRB checks are now called DBS checks.
eGress	A secure email system in use at LBTH. This system can be used as an alternative to GCSX email and should be requested from the ICT Client Team if required.
FTPS	This is a secure FTP file transfer mechanism.
GCSx	Government Connect Secure eXtranet

	(GCSx) is a secure communication network and covers all central government departments and agencies.
ICT	Information Communication Technology
Information asset	Any piece or collection of information that has value to the organisation and needs to be protected in terms of its confidentiality, integrity and availability.
Information governance framework	The range of policies and procedures covering information governance and sets out the way our organisation handles information. The framework determines how we collect and store data, and specifies how the data is used and when it can be shared.
Information lifecycle	The stages information goes through its life as a record from creation through to storage, use and eventual disposal.
Integrity of information	Safeguarding the accuracy and completeness of information and processing methods i.e. maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
Physical Asset	Any piece of equipment/hardware, software or service used to facilitate the usage of information assets
PSN	Public Service Network
Sensitive information	Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure, could cause serious harm to the organisation owning it.
SFTP	Secure File Transfer Protocol. This is one of the mechanisms used to transfer files securely.

Back to Top